Site Recovery Manager Administration

vCenter Site Recovery Manager 5.8

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001400-02

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2008–2015 VMware, Inc. All rights reserved. Copyright and trademark information.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About VMware vCenter Site Recovery Manager Administration

VMware vCenter Site Recovery Manager (Site Recovery Manager) is an extension to VMware vCenter Server that delivers a business continuity and disaster recovery solution that helps you plan, test, and run the recovery of vCenter Server virtual machines. Site Recovery Manager can discover and manage replicated datastores, and automate migration of inventory from one vCenter Server instance to another.

Intended Audience

This book is intended for Site Recovery Manager administrators who are familiar with vSphere and its replication technologies, such as host-based replication and replicated datastores. This solution serves the needs of administrators who want to configure protection for their vSphere inventory. It might also be appropriate for users who need to add virtual machines to a protected inventory or to verify that an existing inventory is properly configured for use with Site Recovery Manager.

Updated Information

Site Recovery Manager Administration is updated with each release of the product or when necessary.

This table provides the update history of *Site Recovery Manager Administration*.

Revision	Description
EN-001400-02	■ Corrected the path to SRA downloads on myvmware.com and clarified that you can download certified SRAs from third party sites in "Install Storage Replication Adapters," on page 22. ■ Corrected the syntax of the DR IP Reporter and DR IP Customizer tools in "Report IP Address Mappings for Recovery Plans," on page 68, "Syntax of the DR IP Customizer Tool," on page 69, and "Run DR IP Customizer to Customize IP Properties for Multiple Virtual Machines," on page 78. ■ Added that advanced settings are not retained during upgrade or after uninstalling and reinstalling the same product version in "Reconfigure Site Recovery Manager Settings," on page 101. ■ Added "Configure Site Recovery Manager Core Dumps," on page 132.
EN-001400-01	■ Clarified what happens to Site Recovery Manager privileges when you uninstall Site Recovery Manager in "Site Recovery Manager Roles Reference," on page 17. ■ Clarified what happens when per-virtual machine command steps fail in "How Site Recovery Manager Handles Custom Recovery Step Failures," on page 58. ■ Corrected the event names in "Recovery Events," on page 122 and "Storage and Storage Provider Events," on page 123.
EN-001400-00	Initial release.

Site Recovery Manager Privileges, Roles, and Permissions 1

Site Recovery Manager provides disaster recovery by performing operations for users. These operations involve managing objects, such as recovery plans or protection groups, and performing operations, such as replicating or powering off virtual machines. Site Recovery Manager uses roles and permissions so that only users with the correct roles and permissions can perform operations.

Site Recovery Manager adds several roles to vCenter Server, each of which includes privileges to complete Site Recovery Manager and vCenter Server tasks. You assign roles to users to permit them to complete tasks in Site Recovery Manager.

Privilege The right to perform an action, for example to create a recovery plan or to modify a protection group.

Role A collection of privileges. Default roles provide the privileges that certain users require to perform a set of Site Recovery Manager tasks, for example users who manage protection groups or perform recoveries. A user can have at most one role on an object, but roles can be combined if the user belongs to multiple groups that all have roles on the object.

Permission A role granted to a particular user or user group on a specific object. A user or user group is also known as a principal. A permission is a combination of a role, an object, and a principal. For example, a permission is the privilege to modify a specific protection group.

For information about the roles that Site Recovery Manager adds to vCenter Server and the privileges that users require to complete tasks, see "Site Recovery Manager Roles Reference," on page 17.

- How Site Recovery Manager Handles Permissions on page 12

  Site Recovery Manager determines whether a user has permission to perform an operation, such as configuring protection or running the individual steps in a recovery plan. This permission check ensures the correct authentication of the user, but it does not represent the security context in which the operation is performed.

- Site Recovery Manager and the vCenter Server Administrator Role on page 13

  If a user or user group has the vCenter Server administrator role on a vCenter Server instance when you install Site Recovery Manager, that user or user group obtains all Site Recovery Manager privileges.

- Site Recovery Manager and vSphere Replication Roles on page 13

  When you install vSphere Replication with Site Recovery Manager, the vCenter Server administrator role inherits all of the Site Recovery Manager and vSphere Replication privileges.

- Managing Permissions in a Shared Recovery Site Configuration on page 14

  You can configure Site Recovery Manager to use with a shared recovery site. The vCenter Server administrator on the shared recovery site must manage permissions so that each user has sufficient privileges to configure and use Site Recovery Manager, but no user has access to resources that belong to another user.

- Assign Site Recovery Manager Roles and Permissions on page 15

  During installation of Site Recovery Manager, users with the vCenter Server administrator role are granted the administrator role on Site Recovery Manager. At this time, only vCenter Server administrators can log in to Site Recovery Manager, unless they explicitly grant access to other users.

- Site Recovery Manager Roles Reference on page 17

  Site Recovery Manager includes a set of roles. Each role includes a set of privileges, which allow users with those roles to complete different actions.

How Site Recovery Manager Handles Permissions

Site Recovery Manager determines whether a user has permission to perform an operation, such as configuring protection or running the individual steps in a recovery plan. This permission check ensures the correct authentication of the user, but it does not represent the security context in which the operation is performed.

Site Recovery Manager performs operations in the security context of the user ID that is used to connect the sites, or in the context of the ID under which the Site Recovery Manager service is running, for example, the local system ID.

After Site Recovery Manager verifies that a user has the appropriate permissions on the target vSphere resources, Site Recovery Manager performs operations on behalf of users by using the vSphere administrator role.

For operations that configure protection on virtual machines, Site Recovery Manager validates the user permissions when the user requests the operation. Operations require two phases of validation.

1. During configuration, Site Recovery Manager verifies that the user configuring the system has the correct permissions to complete the configuration on the vCenter Server object. For example, a user must have permission to protect a virtual machine and use resources on the secondary vCenter Server instance that the recovered virtual machine uses.
2. The user performing the configuration must have the correct permissions to complete the task that they are configuring. For example, a user must have permissions to run a recovery plan.
   Site Recovery Manager then completes the task on behalf of the user as a vCenter Server administrator.

As a result, a user who completes a particular task, such as a recovery, does not necessarily require permissions to act on vSphere resources. The user only requires the permission to run a recovery in Site Recovery Manager. The role authorizes the action, but the action is performed by Site Recovery Manager acting as an administrator. Site Recovery Manager performs the operations by using the administrator credentials that you provide when you connect the protected and recovery sites.

Site Recovery Manager maintains a database of permissions for internal Site Recovery Manager objects that uses a model similar to the one the vCenter Server uses. Site Recovery Manager verifies its own Site Recovery Manager privileges even on vCenter Server objects. For example, Site Recovery Manager checks for the **Resource.Recovery Use** permission on the target datastore rather than checking multiple low-level permissions, such as **Allocate space**. Site Recovery Manager also verifies the permissions on the remote vCenter Server instance.

To use Site Recovery Manager with vSphere Replication, you must assign vSphere Replication roles to users as well as Site Recovery Manager roles. For information about vSphere Replication roles, see *vSphere Replication Administration*.

Site Recovery Manager and the vCenter Server Administrator Role

If a user or user group has the vCenter Server administrator role on a vCenter Server instance when you install Site Recovery Manager, that user or user group obtains all Site Recovery Manager privileges.

If you assign the vCenter Server administrator role to users or user groups after you install Site Recovery Manager, you must manually assign the Site Recovery Manager roles to those users on Site Recovery Manager objects.

You can assign Site Recovery Manager roles to users or user groups that do not have the vCenter Server administrator role. In this case, those users have permission to perform Site Recovery Manager operations, but they do not have permission to perform all vCenter Server operations.

Site Recovery Manager and vSphere Replication Roles

When you install vSphere Replication with Site Recovery Manager, the vCenter Server administrator role inherits all of the Site Recovery Manager and vSphere Replication privileges.

If you manually assign a Site Recovery Manager role to a user or user group, or if you assign a Site Recovery Manager role to a user or user group that is not a vCenter Server administrator, these users do not obtain vSphere Replication privileges. The Site Recovery Manager roles do not include the privileges of the vSphere Replication roles. For example, the Site Recovery Manager Recovery Administrator role includes the privilege to run recovery plans, including recovery plans that contain vSphere Replication protection groups, but it does not include the privilege to configure vSphere Replication on a virtual machine. The separation of the Site Recovery Manager and vSphere Replication roles allows you to distribute responsibilities between different users. For example, one user with the VRM administrator role is responsible for configuring vSphere Replication on virtual machines, and another user with the Site Recovery Manager Recovery Administrator role is responsible for running recoveries.

In some cases, a user who is not vCenter Server administrator might require the privileges to perform both Site Recovery Manager and vSphere Replication operations. To assign a combination of Site Recovery Manager and vSphere Replication roles to a single user, you can add the user to two user groups.

Example: Assign Site Recovery Manager and vSphere Replication Roles to a User

By creating two user groups, you can grant to a user the privileges of both a Site Recovery Manager role and a vSphere Replication role, without that user being a vCenter Server administrator.

1. Create two user groups.
2. Assign a Site Recovery Manager role to one user group, for example Site Recovery Manager administrator.
3. Assign a vSphere Replication role to the other user group, for example VRM administrator.
4. Add the user to both user groups.

The user has all the privileges of the Site Recovery Manager administrator role and of the VRM administrator role.

Managing Permissions in a Shared Recovery Site Configuration

You can configure Site Recovery Manager to use with a shared recovery site. The vCenter Server administrator on the shared recovery site must manage permissions so that each user has sufficient privileges to configure and use Site Recovery Manager, but no user has access to resources that belong to another user.

In the context of a shared recovery site, a user is the owner of a pair of Site Recovery Manager Server instances. Users with adequate permissions must be able to access the shared recovery site to create, test, and run the recovery plans for their own protected site. The vCenter Server administrator at the shared recovery site must create a separate user group for each user. No user's user accounts can be a member of the vCenter Server Administrators group. The only supported configuration for a shared recovery site is for one organization to manage all of the protected sites and the recovery site.

Caution Certain Site Recovery Manager roles allow users to run commands on Site Recovery Manager Server, so you should assign these roles to trusted administrator-level users only. See "Site Recovery Manager Roles Reference," on page 17 for the list of Site Recovery Manager roles that run commands on Site Recovery Manager Server.

On a shared recovery site, multiple customers share a single vCenter Server instance. In some cases, multiple customers can share a single ESXi host on the recovery site. You can map the resources on the protected sites to shared resources on the shared recovery site. You might share resources on the recovery site if you do not need to keep all of the customers' virtual machines separate, for example if all of the customers belong to the same organization.

You can also create isolated resources on the shared recovery site and map the resources on the protected sites to their own dedicated resources on the shared recovery site. You might use this configuration if you must keep all of the customers' virtual machines separate from each other, for example if all of the customers belong to different organizations.

Guidelines for Sharing User Resources

Follow these guidelines when you configure permissions for sharing user resources on the shared recovery site:

- All users must have read access to all folders of the vCenter Server on the shared recovery site.
- Do not give a user the permission to rename, move, or delete the datacenter or host.
- Do not give a user the permission to create virtual machines outside of the user's dedicated folders and resource pools.
- Do not allow a user to change roles or assign permissions for objects that are not dedicated to the user's own use.
- To prevent unwanted propagation of permissions across different organizations' resources, do not propagate permissions on the root folder, datacenters, and hosts of the vCenter Server on the shared recovery site.

Guidelines for Isolating User Resources

Follow these guidelines when you configure permissions for isolating user resources on the shared recovery site:

- Assign to each user a separate virtual machine folder in the vCenter Server inventory.
  - Set permissions on this folder to prevent any other user from placing their virtual machines in it. For example, set the Administrator role and activate the propagate option for a user on that user's folder. This configuration prevents duplicate name errors that might otherwise occur if multiple users protect virtual machines that have identical names.

- Place all of the user's placeholder virtual machines in this folder, so that they can inherit its permissions.
- Do not assign permissions to access this folder to other users.

- Assign dedicated resource pools, datastores, and networks to each user, and configure the permissions in the same way as for folders.

CAUTION A deployment in which you isolate user resources still assumes trust between the vSphere sites. Even though you can isolate user resources, you cannot isolate the users themselves. This is not a suitable deployment if you must keep all users completely separate.

Viewing Tasks and Events in a Shared Recovery Site Configuration

In the Recent Tasks panel of the vSphere Client, users who have permissions to view an object can see tasks that other users start on that object. All users can see all of the tasks that other users perform on a shared resource. For example, all users can see the tasks that run on a shared host, datacenter, or the vCenter Server root folder.

Events that all of the instances of Site Recovery Manager Server generate on a shared recovery site have identical permissions. All users who can see events from one instance of Site Recovery Manager Server can see events from all Site Recovery Manager Server instances that are running on the shared recovery site.

Assign Site Recovery Manager Roles and Permissions

During installation of Site Recovery Manager, users with the vCenter Server administrator role are granted the administrator role on Site Recovery Manager. At this time, only vCenter Server administrators can log in to Site Recovery Manager, unless they explicitly grant access to other users.

To allow other users to access Site Recovery Manager, vCenter Server administrators must grant them permissions in the Site Recovery Manager interface in the vSphere Web Client. Permission assignments apply on a per-site basis. You must add corresponding permissions on both sites.

Site Recovery Manager requires permissions on vCenter Server objects as well as on Site Recovery Manager objects. To configure permissions on the remote vCenter Server installation, start another instance of the vSphere Web Client. You can change Site Recovery Manager permissions from the same vSphere Web Client instance on both sites after you connect the protected and recovery sites.

Site Recovery Manager augments vCenter Server roles and permissions with additional permissions that allow detailed control over Site Recovery Manager specific tasks and operations. For information about the permissions that each Site Recovery Manager role includes, see "Site Recovery Manager Roles Reference," on page 17.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.
2. In the **Manage** tab, click **Permissions**, then click the **Add Permission** icon.
3. Identify a user or group for the role.
   a. Click **Add** in the Users and Groups column.
   b. From the **Domain** drop-down menu, select the domain that contains the user or group.
   c. Enter a user or user group name in the **Search** text box or select a name from the **User/Group** list.
   d. Click **Add** and click **OK**.

4 Select a role from the **Assigned Role** drop-down menu to assign to the user or user group that you selected in Step 3.

The **Assigned Role** drop-down menu includes all of the roles that vCenter Server and its plug-ins make available. Site Recovery Manager adds several roles to vCenter Server.

Option	Action
Allow a user or user group to perform all Site Recovery Manager configuration and administration operations.	Assign the **SRM Administrator** role.
Allow a user or user group to manage and modify protection groups and to configure protection on virtual machines.	Assign the **SRM Protection Groups Administrator** role.
Allow a user or user group to perform recoveries and test recoveries.	Assign the **SRM Recovery Administrator** role.
Allow a user or user group to create, modify, and test recovery plans.	Assign the **SRM Recovery Plans Administrator** role.
Allow a user or user group to test recovery plans.	Assign the **SRM Recovery Test Administrator** role.

When you select a role, the hierarchical list displays the privileges that the role includes. Click a privilege in the hierarchical list to see a description of that privilege. You cannot modify the list of privileges that each role includes.

5 Select **Propagate to Children** to apply the selected role to all of the child objects of the inventory objects that this role can affect.

For example, if a role contains privileges to modify folders, selecting this option extends the privileges to all the virtual machines in a folder. You might deselect this option to create a more complex hierarchy of permissions. For example, deselect this option to override the permissions that are propagated from the root of a certain node from the hierarchy tree, but without overriding the permissions of the child objects of that node.

6 Click **OK** to assign the role and its associated privileges to the user or user group.

7 Repeat Step 2 through Step 6 to assign roles and privileges to the users or user groups on the other Site Recovery Manager site.

You assigned a given Site Recovery Manager role to a user or user group. This user or user group has privileges to perform the actions that the role defines on the objects on the Site Recovery Manager site that you configured.

Example: Combining Site Recovery Manager Roles

You can assign only one role to a user or user group. If a user who is not a vCenter Server administrator requires the privileges of more than one Site Recovery Manager role, you can create multiple user groups. For example, a user might require the privileges to manage recovery plans and to run recovery plans.

1 Create two user groups.

2 Assign the **SRM Recovery Plans Administrator** role to one group.

3 Assign the **SRM Recovery Administrator** role to the other group.

4 Add the user to both user groups.

By being a member of groups that have both the **SRM Recovery Plans Administrator** and the **SRM Recovery Administrator** roles, the user can manage recovery plans and run recoveries.

Site Recovery Manager Roles Reference

Site Recovery Manager includes a set of roles. Each role includes a set of privileges, which allow users with those roles to complete different actions.

Roles can have overlapping sets of privileges and actions. For example, the Site Recovery Manager Administrator role and the Site Recovery Manager Protection Groups Administrator have the **Create** privilege for protection groups. With this privilege, the user can complete one aspect of the set of tasks that make up the management of protection groups.

Assign roles to users on Site Recovery Manager objects consistently on both sites, so that protected and recovery objects have identical permissions.

All users must have at least the **System.Read** privilege on the root folders of vCenter Server and the Site Recovery Manager root nodes on both sites.

Note If you uninstall Site Recovery Manager Server, Site Recovery Manager removes the default Site Recovery Manager roles but the Site Recovery Manager privileges remain. You can still see and assign Site Recovery Manager privileges on other roles after uninstalling Site Recovery Manager. This is standard vCenter Server behavior. Privileges are not removed when you unregister an extension from vCenter Server.

Table 1-1. Site Recovery Manager Roles

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
Site Recovery Manager Administrator	The Site Recovery Manager Administrator grants permission to perform all Site Recovery Manager configuration and administration operations. ■ Configure advanced settings. ■ Configure connections. ■ Configure inventory preferences. ■ Configure placeholder datastores. ■ Configure array managers. ■ Manage protection groups. ■ Manage recovery plans. ■ Perform reprotect operations. ■ Configure protection on virtual machines. ■ Edit protection groups. ■ Remove protection groups. Users with this role cannot run recoveries. Only users with the Site Recovery Manager Recovery Administrator role can perform recoveries.	**Site Recovery Manager.Advanced Settings.Modify** **Site Recovery Manager.Array Manager.Configure** **Site Recovery Manager.DiagnosticsExport.Diagnostics. Export** **Site Recovery Manager.Inventory Preferences.Modify** **Site Recovery Manager.Placeholder Datastores.Configure** **Site Recovery Manager.DiagnosticsExport** **Site Recovery Manager.Protection Group.Assign to Plan** **Site Recovery Manager.Protection Group.Create** **Site Recovery Manager.Protection Group.Modify** **Site Recovery Manager.Protection Group.Remove** **Site Recovery Manager.Protection Group.Remove from Plan** **Site Recovery Manager.Recovery History .View Deleted Plans** **Site Recovery Manager.Recovery Plan.Configure** **Site Recovery Manager.Recovery Plan.Create** **Site Recovery Manager.Recovery Plan.Modify** **Site Recovery Manager.Recovery Plan.Remove** **Site Recovery Manager.Recovery Plan.Reprotect** **Site Recovery Manager.Recovery Plan.Test** **Site Recovery Manager.Remote Site.Modify** **Datastore.Replication.Protect** **Datastore.Replication.Unprotect.Stop** **Resource.Recovery Use** **Virtual Machine. SRM Protection.Protect** **Virtual Machine. SRM Protection.Stop**	■ Virtual machines ■ Datastores ■ vCenter Server folders ■ Resource pools ■ Site Recovery Manager service instances ■ Networks ■ Site Recovery Manager folders ■ Protection groups ■ Recovery plans ■ Array managers
Site Recovery Manager Protection Groups Administrator	The Site Recovery Manager Protection Groups Administrator role allows users to manage protection groups. ■ Create protection groups.	**Site Recovery Manager.Protection Group.Create** **Site Recovery Manager.Protection Group.Modify** **Site Recovery Manager.Protection Group.Remove** **Datastore.Replication.Protect** **Datastore.Replication.Unprotect.Stop** **Resource.Recovery Use**	■ Site Recovery Manager folders ■ Protection groups

Table 1-1. Site Recovery Manager Roles (Continued)

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
	■ Modify protection groups. ■ Add virtual machines to protection groups. ■ Delete protection groups. ■ Configure protection on virtual machines. ■ Remove protection from virtual machines. Users with this role cannot perform or test recoveries or create or modify recovery plans.	**Virtual Machine. SRM Protection.Protect** **Virtual Machine. SRM Protection.Stop**	
Site Recovery Manager Recovery Administrator	The Site Recovery Manager Recovery Administrator role allows users to perform recoveries and reprotect operations. ■ Remove protection groups from recovery plans. ■ Test recovery plans. ■ Run recovery plans. ■ Run reprotect operations. ■ Configure custom command steps on virtual machines. ■ View deleted recovery plans. ■ Edit virtual machine recovery properties. Users with this role cannot configure protection on virtual machines, or create or modify recovery plans.	**Site Recovery Manager.Protection Group.Remove from plan** **Site Recovery Manager.Recovery Plan.Modify** **Site Recovery Manager.Recovery Plan.Test** **Site Recovery Manager.Recovery Plan.Recovery** **Site Recovery Manager.Recovery Plan.Reprotect** **Site Recovery Manager.Recovery Plan.Configure.Configure commands** **Site Recovery Manager.Recovery History.View deleted plans**	■ Protection groups ■ Recovery plans ■ Site Recovery Manager service instances

Table 1-1. Site Recovery Manager Roles (Continued)

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
Site Recovery Manager Recovery Plans Administrator	The Site Recovery Manager Recovery Plans Administrator role allows users to create and test recovery plans. ■ Add protection groups to recovery plans. ■ Remove protection groups from recovery plans. ■ Configure custom command steps on virtual machines. ■ Create recovery plans. ■ Test recovery plans. ■ Cancel recovery plan tests. ■ Edit virtual machine recovery properties. Users with this role cannot configure protection on virtual machines, or perform recoveries or reprotect operations.	**Site Recovery Manager.Protection Group.Assign to plan** **Site Recovery Manager.Protection Group.Remove from plan** **Site Recovery Manager.Recovery Plan.Configure Commands** **Site Recovery Manager.Recovery Plan.Create** **Site Recovery Manager.Recovery Plan.Modify** **Site Recovery Manager.Recovery Plan.Remove** **Site Recovery Manager.Recovery Plan.Test** **Resource.Recovery Use**	■ Protection groups ■ Recovery plans ■ vCenter Server folders ■ Datastores ■ Resource pools ■ Networks
Site Recovery Manager Test Administrator	The Site Recovery Manager Test Administrator role only allows users to test recovery plans. ■ Test recovery plans. ■ Cancel recovery plan tests. ■ Edit virtual machine recovery properties. Users with this role cannot configure protection on virtual machines, create protection groups or recovery plans, or perform recoveries or reprotect operations.	**Site Recovery Manager.Recovery Plan.Modify** **Site Recovery Manager.Recovery Plan.Test**	Recovery plans

Replicating Virtual Machines 2

Before you create protection groups, you must configure replication on the virtual machines to protect.

You can replicate virtual machines by using either array-based replication, vSphere Replication, or a combination of both.

This chapter includes the following topics:

Using Array-Based Replication with Site Recovery Manager

When you use array-based replication, one or more storage arrays at the protected site replicate data to peer arrays at the recovery site. With storage replication adapters (SRAs), you can integrate Site Recovery Manager with a wide variety of arrays.

To use array-based replication with Site Recovery Manager, you must configure replication first before you can configure Site Recovery Manager to use it.

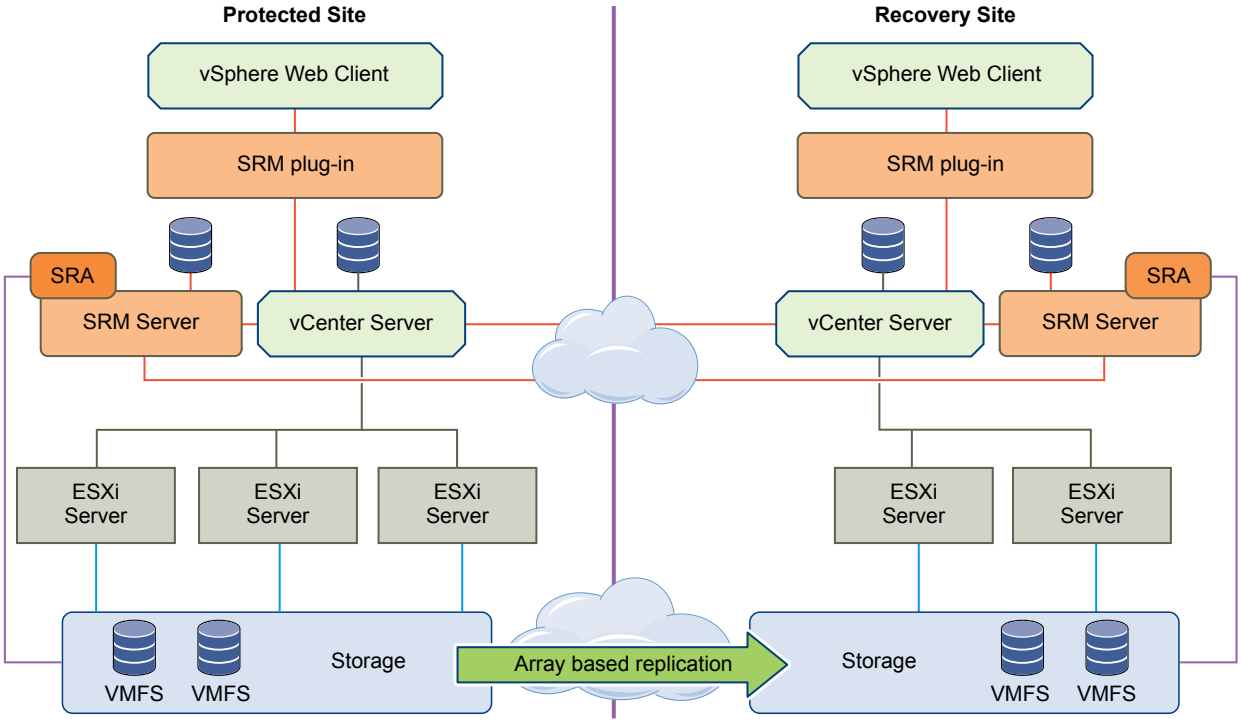
If your storage array supports consistency groups, Site Recovery Manager is compatible with vSphere Storage DRS and vSphere Storage vMotion. You can use Storage DRS and Storage vMotion to move virtual machine files within a consistency group that Site Recovery Manager protects. If your storage array does not support consistency groups, you cannot use Storage DRS and Storage vMotion in combination with Site Recovery Manager.

You can protect virtual machines that contain disks that use VMware vSphere Flash Read Cache storage. Since the host to which a virtual machine recovers might not be configured for Flash Read Cache, Site Recovery Manager disables Flash Read Cache on disks when it starts the virtual machines on the recovery site. Site Recovery Manager sets the reservation to zero. Before performing a recovery on a virtual machine that is configured to use vSphere Flash Read Cache, take a note of virtual machine's cache reservation from the vSphere Web Client. After the recovery, you can migrate the virtual machine to a host with Flash Read Cache storage and manually restore the original Flash Read Cache setting on the virtual machine.

Storage Replication Adapters

Storage replication adapters are not part of a Site Recovery Manager release. Your array vendor develops and supports them. You must install an SRA specific to each array that you use with Site Recovery Manager on the Site Recovery Manager Server host. Site Recovery Manager supports the use of multiple SRAs.

Figure 2-1. Site Recovery Manager Architecture with Array-Based Replication



Configure Array-Based Replication

To protect virtual machines that you replicate by using array-based replication, you must configure storage replication adapters (SRAs) at each site.

Install Storage Replication Adapters

If you are using array-based replication, you must install a Storage Replication Adapter (SRA) specific to each storage array that you use with Site Recovery Manager. An SRA is a program that an array vendor provides that enables Site Recovery Manager to work with a specific kind of array.

You must install an appropriate SRA on the Site Recovery Manager Server hosts at the protected and recovery sites. If you use more than one type of storage array, you must install the SRA for each type of array on both of the Site Recovery Manager Server hosts.

NOTE You can configure Site Recovery Manager to use more than one type of storage array, but you cannot store the virtual machine disks for a single virtual machine on multiple arrays from different vendors. You must store all of the disks for a virtual machine on the same array.

Storage replication adapters come with their own installation instructions. You must install the version of an SRA that corresponds to a specific Site Recovery Manager version. Install the same version of the SRA at both sites. Do not mix SRA versions.

If you are using vSphere Replication, you do not require an SRA.

Prerequisites

- Check the availability of an SRA for your type of storage by consulting the *VMware Compatibility Guide* for Site Recovery Manager at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.

- Download the SRA by going to https://my.vmware.com/web/vmware/downloads, selecting **VMware vCenter Site Recovery Manager > Download Product**, then selecting **Drivers & Tools > Storage Replication Adapters > Go to Downloads**.
- If you obtain an SRA from a different vendor site, verify that it has been certified for the Site Recovery Manager release you are using by checking the *VMware Compatibility Guide* for Site Recovery Manager at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.
- Read the documentation provided with your SRA. SRAs do not support all features that storage arrays support. The documentation that your SRA provides details what the SRA supports and requires. For example, HP and EMC have detailed physical requirements which must be met for the SRA to perform as expected.
- Install Site Recovery Manager Server before you install the SRAs.
- Your SRA might require the installation of other vendor-provided components. You might need to install some of these components on the Site Recovery Manager Server host. Other components might require only network access by the Site Recovery Manager Server. For the latest information on such requirements, review the release notes and readme files for the SRAs you are installing.
- Enable the storage array's capability to create snapshot copies of the replicated devices. See your SRA documentation.

Procedure

1. Install the SRA on each Site Recovery Manager Server host.

   The installer installs the SRA in `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra`.
2. In the vSphere Web Client, go to **Site Recovery > Sites**, and select a site.
3. In the **Monitor** tab, click **SRAs**, and click the **Rescan SRAs** button.

   This action refreshes SRA information, allowing Site Recovery Manager to discover the SRAs.

Configure Array Managers

After you pair the protected site and recovery site, configure their respective array managers so that Site Recovery Manager can discover replicated devices, compute datastore groups, and initiate storage operations.

You typically configure array managers only once after you connect the sites. You do not need to reconfigure them unless array manager connection information or credentials change, or you want to use a different set of arrays.

Prerequisites

- Connect the sites as described in Connect the Protected and Recovery Sites in *Site Recovery Manager Installation and Configuration*.
- Install SRAs at both sites as described in "Install Storage Replication Adapters," on page 22.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Array Based Replication**.
2. In the **Objects** tab, click the icon to add an array manager.
3. Select from two options:
   - Add a pair of array managers
   - Add a single array manager.

4 Select a site or pair of sites for the array manager and click **Next**.

5 Select the array manager type that you want Site Recovery Manager to use from the **SRA Type** drop-down menu.

   If no manager type appears, rescan for SRAs or check that you have installed an SRA on the Site Recovery Manager Server host.

6 Enter a name for the array in the **Display Name** text box.

   Use a descriptive name that makes it easy for you to identify the storage associated with this array manager.

7 Provide the required information for the type of SRA you selected.

   For more information about how to fill in these text boxes, see the documentation that your SRA vendor provides. Text boxes vary between SRAs, but common text boxes include IP address, protocol information, mapping between array names and IP addresses, and user name and password.

8 Click **Next.**

9 If you chose to add a pair of array managers, configure the array pairs, then click **Next**.

   You can also configure array pairs in the single option mode if the array manager on the peer site is already created.

10 Select the array pairs from the list.

11 Review the configuration and click **Finish**.

12 Repeat steps to configure an array manager for the recovery site, if necessary.

Rescan Arrays to Detect Configuration Changes

By default, Site Recovery Manager checks arrays for changes to device configurations by rescanning arrays every 24 hours. However, you can force an array rescan at any time.

You can reconfgure the frequency with which Site Recovery Manager performs regular array scans by changing the `storage.minDsGroupComputationInterval` option in Advanced Settings. See Change Storage Settings .

Configuring array managers causes Site Recovery Manager to compute datastore groups based on the set of replicated storage devices that it discovers. If you change the configuration of the array at either site to add or remove devices, Site Recovery Manager must rescan the arrays and recompute the datastore groups.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Array Based Replication**.

2 Select an array.

3 In the **Manage** tab, select **Array Pairs**.

   The **Array Pairs** tab provides information about all the storage devices in the array, including the local device name, the device it is paired with, the direction of replication, the protection group to which the device belongs, whether the datastore is local or remote, and the consistency group ID for each SRA device.

4 Right-click an array pair and select **Discover Devices** to rescan the arrays and recompute the datastore groups.

Edit Array Managers

Use the Edit Array Manager wizard to modify an array manager's name or other settings, such as the IP address or user name and password.

For more information about how to fill in the adapter fields, see the documentation that your SRA vendor provides. While fields vary among SRAs, common fields include IP address, protocol information, mapping between array names and IP addresses, and user names and passwords.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Array Based Replication**.

2 Right-click an array and select **Edit Array Manager**.

3 Modify the name for the array in the **Display Name** field.

Use a descriptive name that makes it easy for you to identify the storage associated with this array manager. You cannot modify the array manager type.

4 Modify the adapter information.

These fields are created by the SRA.

5 Enable the array pair and click **Next**.

6 Click **Finish** to complete the modification of the array manager.

Specify an Unreplicated Datastore for Swap Files

Every virtual machine requires a swap file. By default, vCenter Server creates swap files in the same datastore as the other virtual machine files. To prevent Site Recovery Manager from replicating swap files, you can configure virtual machines to create them in an unreplicated datastore.

Under normal circumstances, you should keep the swap files in the same datastore as other virtual machine files. However, you might need to prevent replication of swap files to avoid excessive consumption of network bandwidth. Some storage vendors recommend that you do not replicate swap files. Only prevent replication of swap files if it is absolutely necessary.

NOTE If you are using an unreplicated datastore for swap files, you must create an unreplicated datastore for all protected hosts and clusters at both the protected and recovery sites. The unreplicated datastore must be visible to all hosts in a cluster, otherwise vMotion will not work.

Procedure

1 In the vSphere Web Client, select a host and select **Manage > Settings**.

2 Under **Virtual Machines**, click **Swapfile Location**, and click **Edit**.

3 Select **Use a specific datastore**.

4 Select an unreplicated datastore to contain the swap files and click **OK**.

5 Power off and power on all of the virtual machines on the host.

Resetting the guest operating system is not sufficient. The change of swapfile location takes effect after you power off then power on the virtual machines.

6 Browse the datastore that you selected for swapfiles and verify that VSWP files are present for the virtual machines.

Using vSphere Replication with Site Recovery Manager

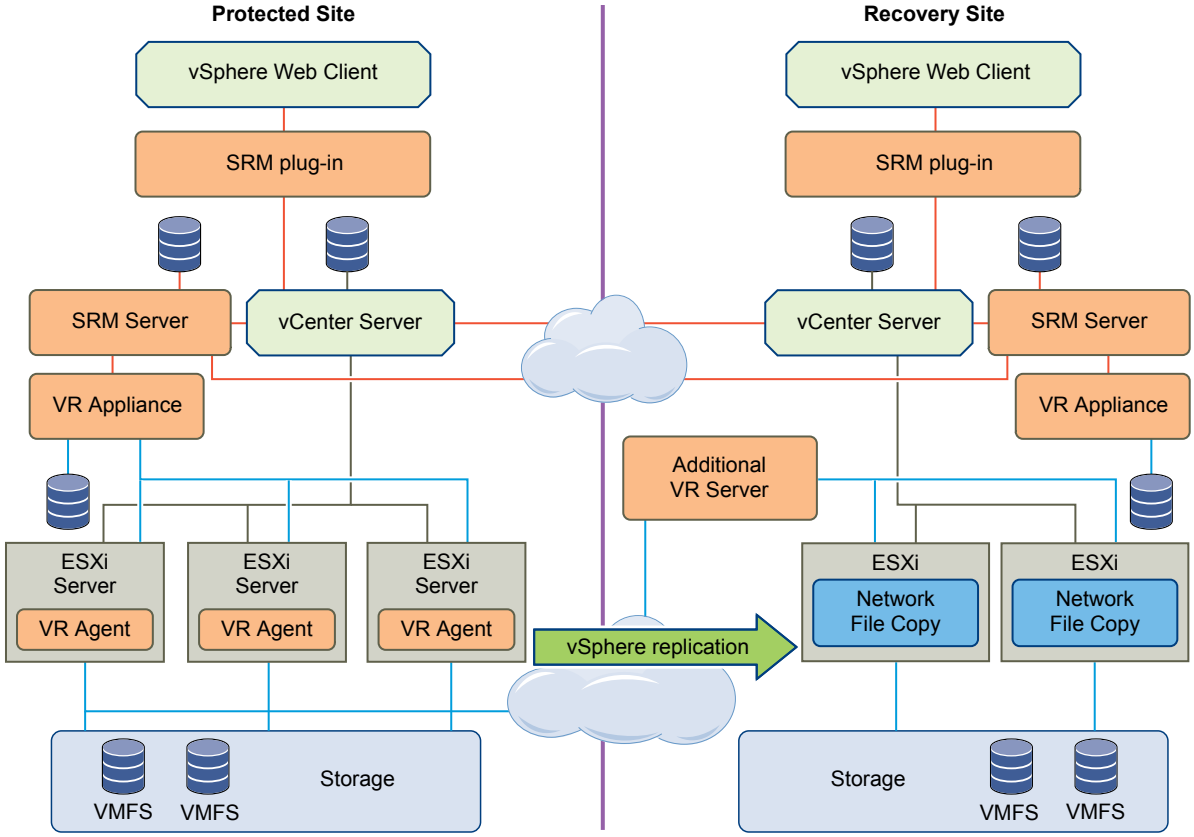
Site Recovery Manager can use vSphere Replication to replicate data to servers at the recovery site.

Previous versions of Site Recovery Manager included the vSphere Replication appliance. In previous releases you could configure vSphere Replication in the Site Recovery Manager interface. In this release, you deploy the vSphere Replication appliance and configure vSphere Replication on virtual machines independently of Site Recovery Manager. See the vSphere Replication documentation at https://www.vmware.com/support/pubs/vsphere-replication-pubs.html for information about deploying and configuring vSphere Replication.

vSphere Replication does not require storage arrays. The vSphere Replication storage replication source and target can be any storage device, including, but not limited to, storage arrays.

You can configure vSphere Replication to regularly create and retain snapshots of protected virtual machines on the recovery site. Taking multiple point-in-time (PIT) snapshots of virtual machines allows you to retain more than one replica of a virtual machine on the recovery site. Each snapshot reflects the state of the virtual machine at a certain point in time. You can select which snapshot to recover when you use vSphere Replication to perform a recovery.

Figure 2-2. Site Recovery Manager Architecture with vSphere Replication



Using vSphere Replication and Site Recovery Manager with vSphere Storage vMotion and vSphere Storage DRS

vSphere Replication is compatible with vSphere Storage vMotion and vSphere Storage DRS on the protected site. You can use Storage vMotion and Storage DRS to move the disk files of a virtual machine that vSphere Replication protects, with no impact on replication.

Using vSphere Replication and VMware Virtual SAN Storage with Site Recovery Manager

You can use VMware Virtual SAN storage with vSphere Replication and Site Recovery Manager.

Replicating a Virtual Machine and Enabling Multiple Point in Time Instances

You can recover virtual machines at specific points in time (PIT) such as the last known consistent state.

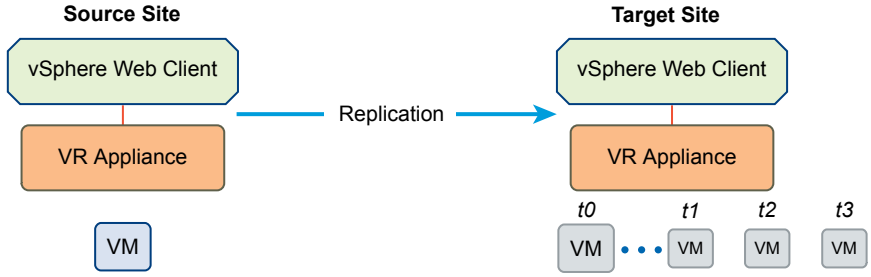
When you configure vSphere Replication on a virtual machine, you can enable the retention of multiple point in time (PIT) instances in the recovery settings. vSphere Replication retains a number of snapshot instances of the virtual machine on the target site based on the retention policy that you specify. vSphere Replication supports maximum of 24 snapshot instances. After you recover a virtual machine, you can revert it to a specific snapshot.

During replication, vSphere Replication replicates all aspects of the virtual machine to the target site, including any potential viruses and corrupted applications. If a virtual machine suffers from a virus or corruption and you have configured vSphere Replication to keep PIT snapshots, you can recover the virtual machine and then revert it to a snapshot of the virtual machine in its uncorrupted state.

For example, you can use the PIT instances to recover the last known good state of a database.

NOTE vSphere Replication does not replicate virtual machine snapshots.

Figure 2-3. Recovering a Virtual Machine at Points in Time (PIT)



Site Recovery Manager only recovers the most recent PIT snapshot during a recovery. To recover older snapshots, you must enable the **vrReplication > preserveMpitImagesAsSnapshots** option in **Advanced Settings** in the Site Recovery Manager interface. See "Change vSphere Replication Settings," on page 110.

To recover a virtual machine from an older PIT snapshot, you must manually revert the virtual machine to that snapshot after the recovery. See "Recover a Point-in-Time Snapshot of a Virtual Machine," on page 50.

If you recover a PIT snapshot of a virtual machine for which you have configured IP customization, Site Recovery Manager only applies the customization to the most recent PIT snapshot. If you recover an older PIT snapshot of a virtual machine with IP customization, you must configure the IP settings manually.

Using Array-Based Replication and vSphere Replication with Site Recovery Manager

You can use a combination of array-based replication and vSphere Replication in your Site Recovery Manager deployment.

To create a mixed Site Recovery Manager deployment that uses array-based replication and vSphere Replication, you must configure the protected and recovery sites for both types of replication.

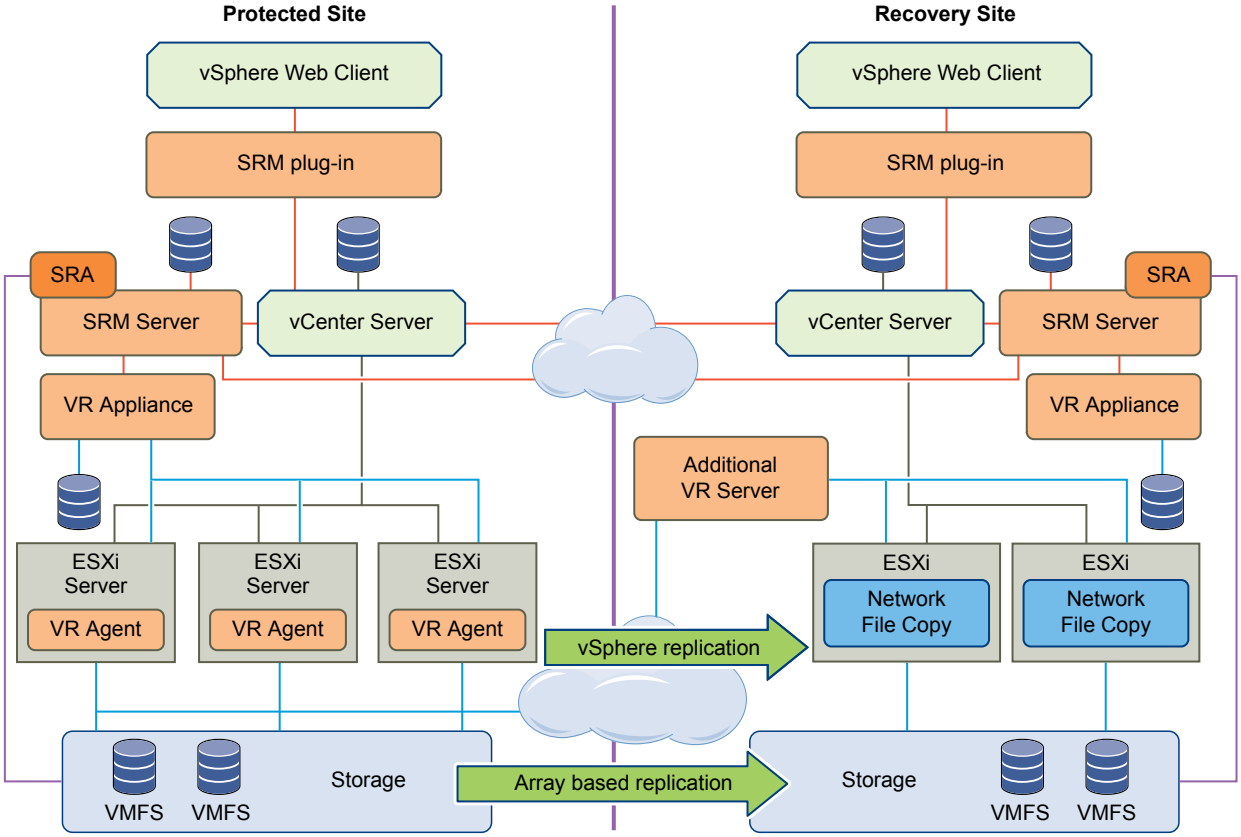
- Set up and connect the storage arrays and install the appropriate storage replication adapters (SRA) on both sites.

- Deploy vSphere Replication appliances on both sites and configure the connection between the appliances.
- Configure virtual machines for replication using either array-based replication or vSphere Replication, as appropriate.

NOTE Do not attempt to configure vSphere Replication on a virtual machine that resides on a datastore that you replicate by using array-based replication.

You create array-based protection groups for virtual machines that you configure with array-based replication, and vSphere Replication protection groups for virtual machines that you configure with vSphere Replication. You cannot mix replication types in a protection group. You can mix array-based protection groups and vSphere Replication protection groups in the same recovery plan.

Figure 2-4. Site Recovery Manager Architecture with Array-Based Replication and vSphere Replication



Creating and Managing Protection Groups

3

After you configure a replication solution, you can create protection groups. A protection group is a collection of virtual machines that Site Recovery Manager protects together.

You can include one or more protection groups in a recovery plan. A recovery plan specifies how Site Recovery Manager recovers the virtual machines in the protection groups that it contains.

You configure virtual machines and create protection groups differently depending on whether you use array-based replication or vSphere Replication. You cannot create protection groups that combine virtual machines for which you configured array-based replication with virtual machines for which you configured vSphere Replication. You can include a combination of array-based protection groups and vSphere Replication protection groups in the same recovery plan.

After you configure replication on virtual machines, you must assign each virtual machine to an existing resource pool, folder, and network on the recovery site. You can specify site-wide defaults for these assignments by selecting inventory mappings. If you do not specify inventory mappings, configure mappings individually for each virtual machine in the protection group.

After you create a protection group, Site Recovery Manager creates placeholder virtual machines on the recovery site and applies the inventory mappings to each virtual machine in the group. If Site Recovery Manager cannot map a virtual machine to a folder, network, or resource pool on the recovery site, Site Recovery Manager sets the virtual machine to the Mapping Missing status, and does not create a placeholder for it.

Site Recovery Manager cannot protect virtual machines on which you did not configure or on which you incorrectly configured replication. In the case of array-based replication, this is true even if the virtual machines reside on a protected datastore.

- Apply Inventory Mappings to All Members of a Protection Group on page 35

  If the status of a protection group is Not Configured, you can configure protection for all of the unconfigured virtual machines by using existing site-wide inventory mappings, in one step.

- Configure Inventory Mappings for an Individual Virtual Machine in a Protection Group on page 36

  You can configure the mappings for the virtual machines in a protection group individually. This ability allows you to use different resources on the recovery site for different virtual machines.

- Modifying the Settings of a Protected Virtual Machine on page 37

  You can edit the settings of a virtual machine in a protection group. Editing the settings of a virtual machine to add or change storage devices, such as hard disks or DVD drives, can affect the protection of that virtual machine.

- Remove Protection from a Virtual Machine on page 38

  You can temporarily remove protection from a replicated virtual machine without removing it from its protection group.

- Protection Group Status Reference on page 38

  You can monitor the status of a protection group and determine the operation that is allowed in each state.

- Virtual Machine Protection Status Reference on page 39

  You can monitor the status of a virtual machine in a protection group and determine the operation that is allowed in each state.

About Array-Based Protection Groups and Datastore Groups

When you create a protection group for array-based replication, you specify array information and Site Recovery Manager computes the set of virtual machines to a datastore group. Datastore groups contain all the files of the protected virtual machines.

You add virtual machines to an array-based protection group by placing them in a datastore that belongs to a datastore group that Site Recovery Manager associates with a protection group. Site Recovery Manager recomputes the datastore groups when it detects a change in a protected virtual machine. For example, if you add a hard disk that is on another LUN to a protected virtual machine, Site Recovery Manager adds the LUN to the datastore group of that protection group. You must reconfigure the protection to protect the new LUN. Site Recovery Manager computes consistency groups when you configure an array pair or when you refresh the list of devices.

You can also add virtual machines to the protection group by using Storage vMotion to move their files to one of the datastores in the datastore group. You can remove a virtual machine from an array-based protection group by moving the virtual machine's files to another datastore.

If your storage array supports consistency groups, Site Recovery Manager is compatible with vSphere Storage DRS and vSphere Storage vMotion. You can use Storage DRS and Storage vMotion to move virtual machine files within a consistency group that Site Recovery Manager protects. If your storage array does not support consistency groups, you cannot use Storage DRS and Storage vMotion in combination with Site Recovery Manager.

How Site Recovery Manager Computes Datastore Groups

Site Recovery Manager determines the composition of a datastore group by the set of virtual machines that have files on the datastores in the group, and by the devices on which those datastores are stored.

When you use array-based replication, each storage array supports a set of replicated datastores. On storage area network (SAN) arrays that use connection protocols such as Fibre Channel and iSCSI, these datastores are called logical storage units (LUN) and are composed of one or more physical datastores. On network file system (NFS) arrays, the replicated datastores are typically referred to as volumes. In every pair of

replicated storage devices, one datastore is the replication source and the other is the replication target. Data written to the source datastore is replicated to the target datastore on a schedule controlled by the replication software of the array. When you configure Site Recovery Manager to work with a storage replication adapter (SRA), the replication source is at the protected site and the replication target is at the recovery site.

A datastore provides storage for virtual machine files. By hiding the details of physical storage devices, datastores simplify the allocation of storage capacity and provide a uniform model for meeting the storage needs of virtual machines. Because any datastore can span multiple devices, Site Recovery Manager must ensure that all devices backing the datastore are replicated before it can protect the virtual machines that use that datastore. Site Recovery Manager must ensure that all datastores containing protected virtual machine files are replicated. During a recovery or test, Site Recovery Manager must handle all such datastores together.

To achieve this goal, Site Recovery Manager aggregates datastores into datastore groups to accommodate virtual machines that span multiple datastores. Site Recovery Manager regularly checks and ensures that datastore groups contain all necessary datastores to provide protection for the appropriate virtual machines. When necessary, Site Recovery Manager recalculates datastore groups. For example, this can occur when you add new devices to a virtual machine, and you store those devices on a datastore that was not previously a part of the datastore group.

A datastore group consists of the smallest set of datastores required to ensure that if any of a virtual machine's files is stored on a datastore in the group, all of the virtual machine's files are stored on datastores that are part of the same group. For example, if a virtual machine has disks on two different datastores, then Site Recovery Manager combines both datastores into a datastore group. Site Recovery Manager combines devices into datastore groups according to set criteria.

- Two different datastores contain files that belong to the same virtual machine.
- Datastores that belong to two virtual machines share a raw disk mapping (RDM) device on a SAN array, as in the case of a Microsoft cluster server (MSCS) cluster.
- Two datastores span extents corresponding to different partitions of the same device.
- A single datastore spans two extents corresponding to partitions of two different devices. The two extents must be in a single consistency group and the SRA must report consistency group information from the array in the device discovery stage. Otherwise, the creation of protection groups based on this datastore is not possible even though the SRA reports that the extents that make up this datastore are replicated.
- Multiple datastores belong to a consistency group. A consistency group is a collection of replicated datastores where every state of the target set of datastores existed at a specific time as the state of the source set of datastores. Informally, the datastores are replicated together such that when recovery happens using those datastores, software accessing the targets does not see the data in a state that the software is not prepared to deal with.

Protecting Virtual Machines on VMFS Datastores that Span Multiple LUNs or Extents

Not all SRAs report consistency group information from the storage array, because not all storage arrays support consistency groups. If an SRA reports consistency group information from the array following a datastore discovery command, the LUNs that constitute a multi-extent VMFS datastore must be in the same storage array consistency group. If the array does not support consistency groups and the SRA does not report any consistency group information, Site Recovery Manager cannot protect virtual machines located on the multi-extent datastore.

About vSphere Replication Protection Groups

You can include virtual machines that you configured for vSphere Replication in vSphere Replication protection groups.

Virtual machines in the vCenter Server inventory that are configured for vSphere Replication are available for selection when you create or edit a vSphere Replication protection group.

You select a location for the replica virtual machine on the target site when you configure vSphere Replication on a virtual machine. When you include a virtual machine with vSphere Replication in a protection group, Site Recovery Manager creates a placeholder virtual machine for recovery. The replica virtual machine that vSphere Replication creates and the placeholder virtual machine that Site Recovery Manager creates can both reside on the same datastore on the recovery site because they are created in different datastore folders. When the replica and placeholder virtual machines are in the same datastore, Site Recovery Manager creates the placeholder virtual machine name by using the replica virtual machine name with the suffix `(1)`. Site Recovery Manager applies the inventory mappings to the placeholder virtual machine on the recovery site.

vSphere Replication synchronizes the disk files of the replica virtual machine according to the recovery point objective that you set when you configured vSphere Replication on the virtual machine. When you perform a recovery with Site Recovery Manager, Site Recovery Manager powers on the replica virtual machine and registers it with vCenter Server on the recovery site in the place of the placeholder virtual machine.

When using vSphere Replication protection groups, Site Recovery Manager is dependent on vSphere Replication, but vSphere Replication is not dependent on Site Recovery Manager. You can use vSphere Replication independently of Site Recovery Manager. For example, you can use vSphere Replication to replicate all of the virtual machines in the vCenter Server inventory, but only include a subset of those virtual machines in protection groups. Changes that you make to vSphere Replication configuration can affect the Site Recovery Manager protection of the virtual machines that you do include in protection groups.

- Site Recovery Manager monitors the vSphere Replication status of the virtual machines in vSphere Replication protection groups. If replication is not functioning for a virtual machine in a protection group, Site Recovery Manager cannot recover the virtual machine.
- If you unconfigure vSphere Replication on a virtual machine, Site Recovery Manager continues to include that virtual machine in protection groups in which you included it. Site Recovery Manager cannot recover that virtual machine until you reconfigure replication. If you unconfigure vSphere Replication on a virtual machine, you can remove it from the protection group manually.
- If you configured vSphere Replication on a virtual machine that resides on a datastore that Site Recovery Manager already protects with array-based replication, Site Recovery Manager reports an error if you try to include that virtual machine in a vSphere Replication protection group.

If you remove a virtual machine with vSphere Replication from a protection group, vSphere Replication continues to replicate the virtual machine to the recovery site. The virtual machine does not recover with the rest of the virtual machines in the protection group if you run an associated recovery plan.

Create Protection Groups

You create protection groups to enable Site Recovery Manager to protect virtual machines.

You can organize protection groups in folders. Different views in the vSphere Web Client display the names of the protection groups, but they do not display the folder names. If you have two protection groups with the same name in different folders, it might be difficult to tell them apart in some views in the vSphere Web Client. Consequently, ensure that protection group names are unique across all folders. In environments in which not all users have view privileges for all folders, to be sure of the uniqueness of protection group names, do not place protection groups in folders.

When you create protection groups, wait to ensure that the operations finish as expected. Make sure that Site Recovery Manager creates the protection group and that the protection of the virtual machines in the group is successful.

Prerequisites

Verify that you performed one of the following tasks:

- Included virtual machines in datastores for which you configured array-based replication
- Configured vSphere Replication on virtual machines
- Performed a combination of both

Procedure

1 In the vSphere Web Client, click **Site Recovery > Protection Groups**.

2 On the **Objects** tab, click the icon to create a protection group.

3 On the Name and location page, enter a name for the protection group, select a pair of sites or a folder, and click **Next**.

4 On the Protection group type page, select the protected site, select the replication type, and click **Next**.

Option	Action
Array-based replication groups	Select **Array Based Replication (ABR)** and select an array pair.
vSphere Replication protection groups	Select **vSphere Replication**.

5 Select datastore groups or virtual machines to add to the protection group.

Option	Action
Array-based protection groups	Select datastore groups and click **Next**.
vSphere Replication protection groups	Select virtual machines from the list, and click **Next**.

When you create vSphere Replication protection groups, only virtual machines that you configured for vSphere Replication and that are not already in a protection group appear in the list.

6 (Optional) Enter a description for the protection group, and click **Next**.

7 Review your settings and click **Finish**.

You can monitor the progress of the creation of the protection group on the **Objects** tab under **Protection Groups**.

- If Site Recovery Manager successfully applied inventory mappings to the protected virtual machines, the status of the protection group is OK.
- If you did not configure inventory mappings, or if Site Recovery Manager was unable to apply them, the status of the protection group is Not Configured.

What to do next

If the status of the protection group is Not Configured, apply inventory mappings to the virtual machines:

- To apply site-wide inventory mappings, or to check that inventory mappings that you have already set are valid, see Select Inventory Mappings in *Site Recovery Manager Installation and Configuration*. To apply these mappings to all of the virtual machines, see "Apply Inventory Mappings to All Members of a Protection Group," on page 35.

- To apply inventory mappings to each virtual machine in the protection group individually, see "Configure Inventory Mappings for an Individual Virtual Machine in a Protection Group," on page 36.

Add or Remove Datastore Groups or Virtual Machines to or from a Protection Group

You can add or remove datastore groups in an array-based protection group, or add or remove virtual machines in a vSphere Replication protection group. You can also change the name and description of a protection group.

Prerequisites

You created a protection group.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Protection Groups**.
2. Right-click a protection group and select **Edit Protection Group**.
3. (Optional) Change the name of the protection group and click **Next**.

   You cannot change the Location setting.
4. Click **Next**.

   You cannot change the Protected Site or Replication Type settings. For array-based protection groups, you cannot change the array pair.
5. Modify the datastore groups or virtual machines that the protection group contains.
   - For array-based protection groups, select or deselect datastore groups to add them to or remove them from the protection group, and click **Next**.
   - For vSphere Replication protection groups, select or deselect virtual machines to add them to or remove them from the protection group, and click **Next**.
6. (Optional) Enter a description for the protection group, and click **Next**.
7. Review the settings and click **Next** to apply the settings.

   You cannot revert or cancel the changes while Site Recovery Manager updates the protection group.
8. Click **Finish** to close the wizard.

- If you configured site-wide inventory mappings, Site Recovery Manager applies the mappings to the virtual machines that you added to the protection group. If successful, the status for the virtual machines is OK.

  NOTE When you add datastores or virtual machines to a protection group, inventory mappings only apply to the new virtual machines. For example, if you change inventory mappings, then add a datastore to a protection group that is in the OK state, Site Recovery Manager applies the new mappings to the newly protected virtual machines that reside in the new datastore. The previously protected virtual machines continue to use the old mappings.

- If you have not configured site-wide inventory mappings, the status for the protection group is Not Configured and the status for the new virtual machines is Mapping Missing.

What to do next

If the status of the protection group is Not Configured and the status for the new virtual machines is Mapping Missing, apply inventory mappings to the virtual machines:

- To apply site-wide inventory mappings, or to check that inventory mappings that you have already set are valid, see Select Inventory Mappings in *Site Recovery Manager Installation and Configuration*. To apply these mappings to all of the virtual machines, see "Apply Inventory Mappings to All Members of a Protection Group," on page 35.
- To apply inventory mappings to each virtual machine in the protection group individually, see "Configure Inventory Mappings for an Individual Virtual Machine in a Protection Group," on page 36.

Apply Inventory Mappings to All Members of a Protection Group

If the status of a protection group is Not Configured, you can configure protection for all of the unconfigured virtual machines by using existing site-wide inventory mappings, in one step.

Site Recovery Manager applies site-wide inventory mappings to virtual machines when you create a protection group or when you add virtual machines to an existing protection group. If you change the site-wide inventory mappings after you create a protection group or add virtual machines to it, the virtual machines continue to recover with the original inventory mappings. To apply new inventory mappings, you must reconfigure protection on the virtual machines in the protection group.

The status of a protection group can be Not Configured for several reasons:

- You did not configure site-wide inventory mappings before you created the protection group.
- You did not configure placeholder datastore mappings before you created the protection group.
- You added virtual machines to a protection group after you created it.
- Virtual machines lost their protection, possibly because you reconfigured them after you added them to a protection group. For example, you added or removed virtual disks or devices.

Prerequisites

- Configure or reconfigure site-wide inventory mappings. To select inventory mappings, see Select Inventory Mappings in *Site Recovery Manager Installation and Configuration*.
- Configure or reconfigure placeholder datastore mappings. To configure a placeholder datastore, see Configure a Placeholder Datastore in *Site Recovery Manager Installation and Configuration*.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Protection Groups**.
2. Select a protection group and on the **Related Objects** tab, click the **Virtual Machines** tab.
3. Click the **Configure All** icon.

   At least one virtual machine in the protection group must be in the Not Configured state for the **Configure All** button to be activated.
4. Click **Yes** to confirm that you want to apply inventory mappings to all unconfigured virtual machines.
   - If Site Recovery Manager successfully applied inventory mappings to the virtual machines, the status of the protection group is OK.
   - If Site Recovery Manager was unable to apply some or all of the inventory mappings, the status of the virtual machines is Not Configured or Mapping Missing.
   - If Site Recovery Manager applied the inventory mappings, but was unable to create placeholders for virtual machines, the status of the virtual machines is Placeholder VM creation error.

5 (Optional) If the status of the virtual machines is Not Configured or Mapping Missing, check the inventory mappings and click **Configure All** again.

6 (Optional) If the status of the virtual machines is Placeholder VM creation error, check the placeholder datastore mapping and try to recreate the placeholder virtual machines.

- To recreate the placeholder for an individual virtual machine, right-click a virtual machine and select **Recreate Placeholder**.
- To recreate the placeholder for several virtual machines, right-click the protection group and select **Restore Placeholder VMs**.

Configure Inventory Mappings for an Individual Virtual Machine in a Protection Group

You can configure the mappings for the virtual machines in a protection group individually. This ability allows you to use different resources on the recovery site for different virtual machines.

You can configure individual inventory mappings even if you configured site-wide inventory mappings. If you did configure site-wide inventory mappings, you can remove protection from an individual virtual machine and configure the folder and resource mappings to override the site-wide mappings. You can change the network mapping for an individual virtual machine without removing protection.

You cannot specify placeholder datastores for individual virtual machines. You must map datastores on the protected site to placeholder datastores on the recovery site at the site level. To configure a placeholder datastore, see Configure a Placeholder Datastore in *Site Recovery Manager Installation and Configuration*.

Prerequisites

You created a protection group.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Protection Groups**.

2 Select the protection group that includes the virtual machine to configure.

3 On the **Related Objects** tab, click the **Virtual Machines** tab.

4 Right-click the virtual machine and select **Configure Protection**.

5 Configure inventory mappings by expanding the resources whose status is Not Configured and selecting resources on the recovery site.

You can only change the folder, resource pool, and network mappings.

6 (Optional) To apply these mappings to all protected virtual machines on the site, select the **Save as Inventory Mapping** check box for each resource.

If you do not select the check box, the mapping is only applied to this virtual machine.

7 Click **OK**.

- If Site Recovery Manager successfully applied inventory mappings to the virtual machine, the status of the virtual machine is OK.
- If Site Recovery Manager was unable to apply some or all of the inventory mappings, the status of the virtual machine is Not Configured or Mapping Missing.
- If Site Recovery Manager applied the inventory mappings but was unable to create a placeholder virtual machine, the status of the virtual machine is Placeholder VM creation error.

8 (Optional) If the status of the virtual machine is Not Configured or Mapping Missing, select **Configure Protection** again and check the inventory mappings.

9 (Optional) If the status of the virtual machine Placeholder VM creation error, check the placeholder datastore mapping at the site level, right-click the virtual machine, and select **Recreate Placeholder**.

Modifying the Settings of a Protected Virtual Machine

You can edit the settings of a virtual machine in a protection group. Editing the settings of a virtual machine to add or change storage devices, such as hard disks or DVD drives, can affect the protection of that virtual machine.

If you use array-based replication, adding or changing devices on a virtual machine affects protection depending on how you create the new device.

- If the new device is on a replicated datastore that is not part of a protection group, the protection group that contains the virtual machine goes into the Not Configured state. Reconfigure the protection group to add the datastore that contains the new device to the protection group.
- If the new device is on a replicated datastore that a different protection group protects, the protection of the virtual machine is invalid.
- If the new device is on an unreplicated datastore, you must replicate the datastore or remove protection from the device.
- If you use Storage vMotion to move a virtual machine to an unreplicated datastore, or to a replicated datastore on an array for which Site Recovery Manager does not have a storage replication adapter (SRA), the protection of the virtual machine is invalid. You can use Storage vMotion to move a virtual machine to datastore that is part of another protection group.

If you add a device to a virtual machine that you protect by using vSphere Replication, you must reconfigure vSphere Replication on the virtual machine to select the replication options for the new device. For information about reconfiguring vSphere Replication settings, see the vSphere Replication documentation at https://www.vmware.com/support/pubs/vsphere-replication-pubs.html.

After you modify virtual machines, you must reconfigure protection for any virtual machines that have a status of Not Configured, Device Not Found, Unresolved Devices, or Mapping Missing. See "Apply Inventory Mappings to All Members of a Protection Group," on page 35 and "Configure Inventory Mappings for an Individual Virtual Machine in a Protection Group," on page 36.

Disabling Replication on a Protected Virtual Machine

All virtual machines in a protection group must be configured for either array-based replication or vSphere Replication. If you disable replication on a virtual machine that is part of a protection group, Site Recovery Manager cannot recover that virtual machine and the status for that protection group is Not Configured.

- If you remove protection from a virtual machine that is part of array-based replication protection group, you must move the files of that virtual machine to an unprotected datastore. If you leave the files of an unprotected virtual machine in a datastore that Site Recovery Manager has included in a datastore group, recovery fails for the entire datastore group.
- If you disable vSphere Replication on a virtual machine that you included in a protection group, recovery fails for this virtual machine but succeeds for all of the correctly configured virtual machines in the group. You must edit the protection group to remove the virtual machine. See "Add or Remove Datastore Groups or Virtual Machines to or from a Protection Group," on page 34.

Remove Protection from a Virtual Machine

You can temporarily remove protection from a replicated virtual machine without removing it from its protection group.

Removing protection deletes the placeholder virtual machine on the recovery site. If you remove protection from a virtual machine, the states of the virtual machine and the protection group are set to Not Configured. Running a recovery plan that contains the protection group succeeds, but Site Recovery Manager does not recover the virtual machines that are in the Not Configured state.

You might remove protection from a virtual machine for different reasons:

- You use vSphere Replication and you want to reconfigure a protected virtual machine. You can remove protection while you reconfigure the virtual machine, so that ongoing Site Recovery Manager test or real recoveries are not affected by the changes. For example, if you add devices to a virtual machine and run a recovery before you configure vSphere Replication on the new devices, the recovery shows errors if you do not remove protection from the virtual machine.
- You use array-based replication, and someone moves to a replicated datastore a virtual machine that you do not want to protect. If you remove protection from the virtual machine, the protection group still shows the Not Configured state, but test recovery and real recovery continue to succeed.
- You use array-based replication and a virtual machine has devices that are stored on an unreplicated datastore. You can remove protection from the virtual machine so that recoveries succeed for all of the other virtual machines in the group while you relocate the device files.
- In array-based replication, a distinction exists between the Site Recovery Manager protection of a virtual machine and the Site Recovery Manager storage management for that virtual machine. If you remove protection from a virtual machine, Site Recovery Manager no longer recovers the virtual machine, but it continues to monitor and manage the storage of the virtual machine files.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Protection Groups**.

2 Select a protection group and select **Related Objects > Virtual Machines**.

3 Right-click a virtual machine and select **Remove Protection**.

4 Click **Yes** to confirm the removal of protection from the virtual machine.

Protection Group Status Reference

You can monitor the status of a protection group and determine the operation that is allowed in each state.

Table 3-1. Protection Group States

State	Description
Loading	Appears briefly while the interface is loading until the protection group status appears.
OK	Group is idle. All virtual machines are in OK state. You can edit the group.
Not Configured	Group is idle. Some virtual machines might not be in OK state. You can edit the group.
Testing	Group is used in a plan running a test. You cannot edit the group.
Test Complete	Group is used in a plan running a test. You cannot edit the group. Group returns to the OK or Not Configured state when cleanup is successful.

Table 3-1. Protection Group States (Continued)

State	Description
Cleaning Up	Group is used in a plan that is cleaning up after a test. You cannot edit the group. Group returns to the OK or Not Configured state when cleanup is successful. If cleanup fails, the group goes to the Testing state.
Recovering	Group is used in a plan that is running a recovery. You cannot edit the group. If recovery succeeds, the group goes to Recovered state. If recovery fails, group status changes to Partially Recovered.
Partially Recovered	Group is in a plan that completed a recovery, but recovery failed for some virtual machines. You can remove virtual machines, but cannot configure or restore them.
Recovered	Group is in a plan that successfully completed a recovery. You can remove virtual machines, but cannot configure or restore them.
Reprotecting	Group is used in a plan running reprotect. You cannot edit the group. Group returns to OK or Not Configured state when reprotect is successful. If reprotect fails, the group goes to Partially Reprotected state.
Partially Reprotected	The group is in a plan that failed a reprotect. You can remove virtual machines, but cannot configure or restore them.
Configuring Protection	Protection operations are in progress on virtual machines in the group.
Removing Protection	Removing protection from virtual machines in the group is in progress.
Restoring Placeholders	Creation of placeholders is in progress for virtual machines in the group.
Operations in Progress	A combination of at least one Configure Protection and one Remove Protection operations are in progress in the group.

Virtual Machine Protection Status Reference

You can monitor the status of a virtual machine in a protection group and determine the operation that is allowed in each state.

Table 3-2. Virtual Machine Protection States

State	Description
Placeholder VM Not Found	You deleted the placeholder virtual machine. The Restore Placeholder icon is enabled.
Original protected VM not found	You deleted the original production virtual machine after failover and before reprotect. The Restore Placeholder icon is enabled.
Datastore *name* used by VM is missing from group	The virtual machine requires a datastore that is not in the protection group. Edit the protection group to include the datastore.
Datastore *name* used by VM is protected in a different group	The virtual machine requires a datastore that is in a different protection group. Remove the datastore from the other protection group and edit the current protection group to include the datastore. You cannot include a datastore in two protection groups.

Table 3-2. Virtual Machine Protection States (Continued)

State	Description
Device not found: *device name*	You added an unreplicated disk or device to a protected virtual machine. You must edit the replication of the virtual machine either include or remove the device from protection.
Mapping missing: Folder *name*; Network *name* ; Resource pool *name*	Folder, resource pool, or network mappings are not configured for this VM. Fix the inventory mappings for the site or manually configure the virtual machine.
Placeholder VM creation error: *error string from server*	Error during placeholder virtual machine creation.
OK	The protected virtual machine exists, and both provider and placeholder status are clean.
Invalid: *error*	The virtual machine is not valid because the home datastore is not replicated or the virtual machine has been deleted. The error string from the server contains the details. Remove protection from the virtual machine manually.
Not configured	You added a new virtual machine after creating the protection group. Use Configure All to configure protection on the virtual machine.
Error: *error*	Error can be one of the following: ■ Recovery site resource pool, folder, or network are not in the same datacenter. ■ Placeholder datastore not found. ■ Any vCenter Server error that occurred when creating placeholder, such as connection or permission problems.
Configuring protection	Virtual machine operation.
Removing protection	Virtual machine operation.
Restoring placeholder	Virtual machine operation.
Loading	Appears briefly while the interface is loading until the virtual machine status appears.
Mapping Conflict	Site Recovery Manager Server reported an inventory conflict. The resource pool and folder of the virtual machine are in different datacenters.
Replication Error	vSphere Replication reports an error about the virtual machine.
Replication Warning	vSphere Replication reports a warning about the virtual machine.

Creating, Testing, and Running Recovery Plans

4

After you configure Site Recovery Manager at the protected and recovery sites, you can create, test, and run a recovery plan.

A recovery plan is like an automated run book. It controls every step of the recovery process, including the order in which Site Recovery Manager powers on and powers off virtual machines, the network addresses that recovered virtual machines use, and so on. Recovery plans are flexible and customizable.

A recovery plan includes one or more protection groups. You can include a protection group in more than one recovery plan. For example, you can create one recovery plan to handle a planned migration of services from the protected site to the recovery site, and another plan to handle an unplanned event such as a power failure or natural disaster. In this example, having these different recovery plans referencing one protection group allows you to decide how to perform recovery. To create a protection group, see "Create Protection Groups," on page 32.

You can run only one recovery plan at a time to recover a particular protection group. If you simultaneously test or run multiple recovery plans that specify the same protection group, only one recovery plan can operate on the protection group. Other running recovery plans that specify the same protection group report warnings for that protection group and the virtual machines it contains. The warnings explain that the virtual machines were recovered, but do not report other protection groups that the other recovery plans cover.

- Export Recovery Plan Steps on page 51

  You can export the steps of a recovery plan in various formats for future reference, or to keep a hard copy backup of your plans.

- View and Export a Recovery Plan History on page 51

  You can view and export reports about each run of a recovery plan, test of a recovery plan, or test cleanup.

- Delete a Recovery Plan on page 52

  You can delete a recovery plan if you do not need it.

- Recovery Plan Status Reference on page 52

  You can monitor the status of a recovery plan and determine the operation that is allowed in each state. The state of a recovery plan is determined by the states of the protection groups within the plan.

Testing a Recovery Plan

When you create or modify a recovery plan, test it before you try to use it for planned migration or for disaster recovery.

By testing a recovery plan, you ensure that the virtual machines that the plan protects recover correctly to the recovery site. If you do not test recovery plans, an actual disaster recovery situation might not recover all virtual machines, resulting in data loss.

Testing a recovery plan exercises nearly every aspect of a recovery plan, although Site Recovery Manager makes several concessions to avoid disrupting ongoing operations on the protected and recovery sites. Recovery plans that suspend local virtual machines do so for tests as well as for actual recoveries. With this exception, running a test recovery does not disrupt replication or ongoing activities at either site.

If you use vSphere Replication, when you test a recovery plan, the virtual machine on the protected site can still synchronize with the replica virtual machine disk files on the recovery site. The vSphere Replication server creates redo logs on the virtual machine disk files on the recovery site, so that synchronization can continue normally. When you perform cleanup after running a test, the vSphere Replication server removes the redo logs from the disks on the recovery site and persists the changes accumulated in the logs to VM disks.

If you use array-based replication, when you test a recovery plan, the virtual machines on the protected site are still replicated to the replica virtual machines' disk files on the recovery site. During test recovery, the array creates a snapshot of the volumes hosting the virtual machines' disk files on the recovery site. Array replication continues normally while the test is in progress. When you perform cleanup after running a test, the array removes the snapshots that were created earlier as part of test recovery workflow.

You can run test recoveries as often as necessary. You can cancel a recovery plan test at any time.

Before running a failover or another test, you must successfully run a cleanup operation. See "Clean Up After Testing a Recovery Plan," on page 48.

Permission to test a recovery plan does not include permission to run a recovery plan. Permission to run a recovery plan does not include permission to test a recovery plan. You must assign each permission separately. See "Assign Site Recovery Manager Roles and Permissions," on page 15.

Test Networks and Datacenter Networks

When you test a recovery plan, Site Recovery Manager can create a test network that it uses to connect recovered virtual machines. Creating a test network allows the test to run without potentially disrupting virtual machines in the production environment.

The test network is managed by its own virtual switch, and in most cases recovered virtual machines can use the network without having to change network properties such as IP address, gateway, and so on. You use the test network by selecting **Auto** when you configure the test network settings while creating a recovery plan. A test network does not span hosts. You must configure a test network for every network that a recovery plan uses during recovery.

You must recover any virtual machines that must interact with each other to the same test network. For example, if a Web server accesses information on a database, those Web server and database virtual machines should recover together to the same network.

A datacenter network is a network that typically supports existing virtual machines at the recovery site. You can select a datacenter network for use as a test network. To use it, recovered virtual machines must conform to its network address availability rules. These virtual machines must use a network address that the network's switch can serve and route, must use the correct gateway and DNS host, and so on. Recovered virtual machines that use DHCP can connect to this network without additional customization. Other virtual machines require IP customization and additional recovery plan steps to apply the customization.

Performing a Planned Migration or Disaster Recovery By Running a Recovery Plan

You can run a recovery plan under planned circumstances to migrate virtual machines from the protected site to the recovery site. You can also run a recovery plan under unplanned circumstances if the protected site suffers an unforeseen event that might result in data loss.

During a planned migration, Site Recovery Manager synchronizes the virtual machine data on the recovery site with the virtual machines on the protected site. Site Recovery Manager attempts to gracefully shut down the protected machines and performs a final synchronization to prevent data loss, then powers on the virtual machines on the recovery site. If errors occur during a planned migration, the plan stops so that you can resolve the errors and rerun the plan. You can reprotect the virtual machines after the recovery.

During disaster recoveries, Site Recovery Manager first attempts a storage synchronization. If it succeeds, Site Recovery Manager uses the synchronized storage state to recover virtual machines on the recovery site to their most recent available state, according to the recovery point objective (RPO) that you set when you configure your replication technology. When you run a recovery plan to perform a disaster recovery, Site Recovery Manager attempts to shut down the virtual machines on the protected site. If Site Recovery Manager cannot shut down the virtual machines, Site Recovery Manager still starts the copies at the recovery site. In case the protected site comes back online after disaster recovery, the recovery plan goes into an inconsistent state where production virtual machines are running on both sites, known as a split-brain scenario. Site Recovery Manager detects this state and allows you to run the plan once more to power off the virtual machines on the protected site. Then the recovery plan goes back to consistent state and you can run reprotect.

If Site Recovery Manager detects that a datastore on the protected site is in the all paths down (APD) state and is preventing a virtual machine from shutting down, Site Recovery Manager waits for a period before attempting to shut down the virtual machine again. The APD state is usually transient, so by waiting for a datastore in the APD state to come back online, Site Recovery Manager can gracefully shut down the protected virtual machines on that datastore.

Site Recovery Manager uses VMware Tools heartbeat to discover when a virtual machine is running on the recovery site. In this way, Site Recovery Manager can ensure that all virtual machines are running on the recovery site. For this reason, VMware recommends that you install VMware Tools on protected virtual machines. If you do not or cannot install VMware Tools on the protected virtual machines, you must configure Site Recovery Manager not to wait for VMware Tools to start in the recovered virtual machines and to skip the guest operating system shutdown step. See "Change Recovery Settings," on page 105.

After Site Recovery Manager completes the final replication, Site Recovery Manager makes changes at both sites that require significant time and effort to reverse. Because of this time and effort, you must assign the privilege to test a recovery plan and the privilege to run a recovery plan separately.

Running a Recovery with Forced Recovery

If the protected site is offline and Site Recovery Manager cannot perform its usual tasks in a timely manner which increases the RTO to unacceptable level, you can run the recovery with the forced recovery option. Forced recovery starts the virtual machines on the recovery site without performing any operations on the protected site.

Caution Only use forced recovery in cases where the recovery time objective (RTO) is severely affected by a lack of connectivity to the protection site.

Forced recovery is for use in cases where infrastructure fails at the protected site and, as a result, protected virtual machines are unmanageable and cannot be shut down, powered off, or unregistered. In such a case, the system state cannot be changed for extended periods. To resolve this situation, you can force recovery. Forcing recovery does not complete the process of shutting down the virtual machines at the protected site. As a result, a split-brain scenario occurs, but the recovery might complete more quickly.

Running disaster recovery with array-based replication when the protected site storage array is offline or unavailable can affect the mirroring between the protected and the recovery storage arrays. After you run forced recovery, you must check that mirroring is set up correctly between the protected array and the recovery array before you can perform further replication operations. If mirroring is not set up correctly, you must repair the mirroring by using the storage array software.

When running disaster recovery using vSphere Replication, Site Recovery Manager prepares vSphere Replication storage for reprotect and you do not have to verify mirroring as you do with array-based replication.

When you enable forced recovery when the protected site storage is still available, any outstanding changes on the protection site are not replicated to the recovery site before the sequence begins. Replication of the changes occurs according to the recovery point objective (RPO) period of the storage array. If a new virtual machine or template is added on the protection site and recovery is initiated before the storage RPO period has elapsed, the new virtual machine or template does not appear on the replicated datastore and is lost. To avoid losing the new virtual machine or template, wait until the end of the RPO period before running the recovery plan with forced recovery.

To select forced recovery when running disaster recovery, you must enable the option `recovery.forceRecovery` in Advanced Settings on the recovery Site Recovery Manager server. In the Run Recovery Plan wizard, select the forced recovery option only in disaster recovery mode. It is not available for planned migration.

After the forced recovery completes and you have verified the mirroring of the storage arrays, you can resolve the issue that necessitated the forced recovery. After you resolve the underlying issue, run planned migration on the recovery plan again, resolve any problems that occur, and rerun the plan until it finishes successfully. Running the recovery plan again does not affect the recovered virtual machines at the recovery site.

Differences Between Testing and Running a Recovery Plan

Testing a recovery plan has no lasting effects on either the protected site or the recovery site, but running a recovery plan has significant effects on both sites.

You need different privileges when testing and running a recovery plan.

Table 4-1. How Testing a Recovery Plan Differs from Running a Recovery Plan

Area of Difference	Test a Recovery Plan	Run a Recovery Plan
Required privileges	Requires **Site Recovery Manager.Recovery Plans.Test** permission.	Requires **Site Recovery Manager.Recovery Plans.Recovery** permission.
Effect on virtual machines at protected site	None	Site Recovery Manager shuts down virtual machines in reverse priority order and restores any virtual machines that are suspended at the protected site.
Effect on virtual machines at recovery site	Site Recovery Manager suspends local virtual machines if the recovery plan requires this. Site Recovery Manager restarts suspended virtual machines after cleaning up the test.	Site Recovery Manager suspends local virtual machines if the recovery plan requires this.
Effect on replication	Site Recovery Manager creates temporary snapshots of replicated storage at the recovery site. For array-based replication, Site Recovery Manager rescans the arrays to discover them.	During a planned migration, Site Recovery Manager synchronizes replicated datastores, then stops replication, then makes the target devices at the recovery site writable. During a disaster recovery, Site Recovery Manager attempts the same steps, but if they do not succeed, Site Recovery Manager ignores protected site errors.
Network	If you explicitly assign test networks, Site Recovery Manager connects recovered virtual machines to a test network. If virtual machine network assignment is **Auto**, Site Recovery Manager assigns virtual machines to temporary networks that are not connected to any physical network.	Site Recovery Manager connects recovered virtual machines to the user-specified datacenter network.
Interruption of recovery plan	You can cancel a test at any time.	You can cancel the recovery at any time.

Performing Test Recovery of Virtual Machines Across Multiple Hosts on the Recovery Site

You can create recovery plans that recover virtual machines across multiple recovery site hosts in a quarantined test network.

With Site Recovery Manager, the vSwitches can be DVS based and span hosts. If you accept the default test network configured as Auto, then virtual machines that are recovered across hosts are placed in their own test network during recovery plan tests. Each test switch is isolated between hosts. As a result, virtual machines in the same recovery plan are isolated when the test recovery finishes. To allow the virtual

machines to communicate, establish and select DVS switches or VLANs. With an isolated VLAN that connects all hosts to each other but not to a production network, you can more realistically test a recovery. To achieve connectivity among recovery hosts, but maintain isolation from the production network, follow these recommendations:

- Create DVS switches that are connected to an isolated VLAN that is private. Such a VLAN allows hosts and virtual machines to be connected, but to be isolated from production virtual machines. Use a naming convention that clearly designates that the DVS is for testing use, and select this DVS in the recovery plan test network column in the recovery plan editor.
- Create test VLANs on a physical network, providing no route back to the protected site. Trunk test VLANs to recovery site vSphere clusters and create virtual switches for test VLAN IDs. Use a clear naming convention to identify that these switches are for testing. Select these switches from the test recovery network column in the recovery plan editor.

Create, Test, and Run a Recovery Plan

You perform several sets of tasks to create, test, and run a recovery plan.

Procedure

1 Create a Recovery Plan on page 46

You create a recovery plan to establish how Site Recovery Manager recovers virtual machines.

2 Edit a Recovery Plan on page 47

You can edit a recovery plan to change the properties that you specified when you created it. You can edit recovery plans from the protected site or from the recovery site.

3 Test a Recovery Plan on page 48

When you test a recovery plan, Site Recovery Manager runs the virtual machines of the recovery plan on a test network and on a temporary snapshot of replicated data at the recovery site.
Site Recovery Manager does not disrupt operations at the protected site.

4 Clean Up After Testing a Recovery Plan on page 48

After you test a recovery plan, you can return the recovery plan to the Ready state by running a cleanup operation. You must complete the cleanup operation before you can run a failover or another test.

5 Run a Recovery Plan on page 49

When you run a recovery plan, Site Recovery Manager migrates all virtual machines in the recovery plan to the recovery site. Site Recovery Manager attempts to shut down the corresponding virtual machines on the protected site.

6 Recover a Point-in-Time Snapshot of a Virtual Machine on page 50

With vSphere Replication, you can retain point-in-time snapshots of a virtual machine. You can configure Site Recovery Manager to recover a number of point-in-time (PIT) snapshots of a virtual machine when you run a recovery plan.

7 Cancel a Test or Recovery on page 51

You can cancel a recovery plan test whenever the status is test in progress or failover in progress.

Create a Recovery Plan

You create a recovery plan to establish how Site Recovery Manager recovers virtual machines.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**.

2 On the **Related Objects > Recovery Plans** tab, click the icon to create a recovery plan.

3 Enter a name for the plan, select a location, then click **Next**.

4 Select the recovery site and click **Next**.

5 Select one or more protection groups for the plan to recover, and click **Next**.

6 Select a test network for the virtual machines whose configured recovery network is the selected recovery network identified by the datacenter and recovery network. The test network can be only from the same datacenter and the default is Auto.

Option	Action
Datacenter	Select the datacenter to which virtual machines recover.
Recovery Network	Select the network to use for planned migration and disaster recovery.
Test Network	Select the test network to use for recovery plan tests.

7 Click **Next**.

8 (Optional) Add a description for the recovery plan and click **Next**.

9 Review the summary information and click **Finish** to create the recovery plan.

Edit a Recovery Plan

You can edit a recovery plan to change the properties that you specified when you created it. You can edit recovery plans from the protected site or from the recovery site.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**.

2 Right-click a recovery plan, and select **Edit Plan**. You can also edit the plan from the Recovery Steps tab.

3 (Optional) Change the name of the plan in the **Recovery Plan Name** text box, and click **Next**.

4 On the Recovery site page, click **Next**.

You cannot change the recovery site.

5 (Optional) Select or deselect one or more protection groups to add them to or remove them from the plan, and click **Next**.

6 (Optional) Change the recovery site test network settings.

a Select the configured network settings and click **Remove**.

b Select a new test network for any recovery network.

7 Click **Next**.

8 (Optional) Enter or modify the description for the plan and click **Next**.

9 Review the summary information and click **Finish** to make the specified changes to the recovery plan.

You can monitor the update of the plan in the Recent Tasks view.

Test a Recovery Plan

When you test a recovery plan, Site Recovery Manager runs the virtual machines of the recovery plan on a test network and on a temporary snapshot of replicated data at the recovery site. Site Recovery Manager does not disrupt operations at the protected site.

Testing a recovery plan runs all the steps in the plan, except for powering down virtual machines at the protected site and forcing devices at the recovery site to assume mastership of replicated data. If the plan requires the suspension of local virtual machines at the recovery site, Site Recovery Manager suspends those virtual machines during the test. Running a test of a recovery plan makes no other changes to the production environment at either site.

Testing a recovery plan creates a snapshot on the recovery site of all of the disk files of the virtual machines in the recovery plan. The creation of the snapshots adds to the I/O latency on the storage. If you notice slower response times when you test recovery plans and you are using VMware Virtual SAN storage, monitor the I/O latency by using the monitoring tool in the Virtual SAN interface.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 Right-click the plan and select **Test**. You can also run the test from the Recovery Steps tab.

3 (Optional) Select **Replicate recent changes to recovery site**.

Selecting this option ensures that the recovery site has the latest copy of protected virtual machines, but the synchronization might take more time.

4 Click **Next**.

5 Review the test information and click **Finish**.

6 Click the **Recovery Steps** tab to monitor the progress of the test and respond to messages.

The **Recovery Steps** tab displays the progress of individual steps. The Test task in Recent Tasks tracks overall progress.

NOTE Site Recovery Manager runs recovery steps in the prescribed order, except that it does not wait for the Prepare Storage step to finish for all protection groups before continuing to the next steps.

What to do next

Run a cleanup operation after the recovery plan test finishes to restore the recovery plan to its original state from before the test.

Clean Up After Testing a Recovery Plan

After you test a recovery plan, you can return the recovery plan to the Ready state by running a cleanup operation. You must complete the cleanup operation before you can run a failover or another test.

Site Recovery Manager performs several cleanup operations after a test.

- Powers off the recovered virtual machines.
- Replaces recovered virtual machines with placeholders, preserving their identity and configuration information.
- Cleans up replicated storage snapshots that the recovered virtual machines used during the test.

Prerequisites

Verify that you tested a recovery plan.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 Right-click the recovery plan and select **Cleanup**. You can also run cleanup from the Recovery Steps tab.

3 Review the cleanup information and click **Next**.

4 Click **Finish**.

5 After the cleanup finishes, if it reports errors, run the cleanup again, selecting the **Force Cleanup** option.

The **Force Cleanup** option forces the removal of virtual machines, ignoring any errors, and returns the plan to the Ready state. If necessary, run cleanup several times with the **Force Cleanup** option, until the cleanup succeeds.

Run a Recovery Plan

When you run a recovery plan, Site Recovery Manager migrates all virtual machines in the recovery plan to the recovery site. Site Recovery Manager attempts to shut down the corresponding virtual machines on the protected site.

CAUTION A recovery plan makes significant alterations in the configurations of the protected and recovery sites and it stops replication. Do not run any recovery plan that you have not tested. Reversing these changes might cost significant time and effort and can result in prolonged service downtime.

Prerequisites

To use forced recovery, you must first enable this function. You enable forced recovery by enabling the **recovery.forceRecovery** setting as described in "Change Recovery Settings," on page 105.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 Right-click the recovery plan and select **Run**.

3 Review the information in the confirmation prompt, and select **I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters**.

4 Select the type of recovery to run.

Option	Description
Planned Migration	Recovers virtual machines to the recovery site when both sites are running. If errors occur on the protected site during a planned migration, the planned migration operation fails.
Disaster Recovery	Recovers virtual machines to the recovery site if the protected site experiences a problem. If errors occur on the protected site during a disaster recovery, the disaster recovery continues and does not fail.

5 (Optional) Select the **Forced Recovery - recovery site operations only** check box.

This option is available if you enabled the forced recovery function and you selected **Disaster Recovery**.

6 Click **Next**.

7 Review the recovery information and click **Finish**.

8 Click the **Monitor** tab and click **Recovery Steps**.

The **Recovery Steps** tab displays the progress of individual steps. The Recent Tasks area reports the progress of the overall plan.

Recover a Point-in-Time Snapshot of a Virtual Machine

With vSphere Replication, you can retain point-in-time snapshots of a virtual machine. You can configure Site Recovery Manager to recover a number of point-in-time (PIT) snapshots of a virtual machine when you run a recovery plan.

You configure the retention of PIT snapshots when you configure vSphere Replication on a virtual machine. For more information about PIT snapshots, see "Replicating a Virtual Machine and Enabling Multiple Point in Time Instances," on page 27.

To enable PIT snapshots, configure replication of a virtual machine by using the vSphere Replication interface in the vSphere Web Client.

Site Recovery Manager only recovers the most recent PIT snapshot during a recovery. To recover older snapshots, you must enable the `vrReplication > preserveMpitImagesAsSnapshots` option in Advanced Settings in the Site Recovery Manager interface. If you recover a PIT snapshot of a virtual machine for which you have configured IP customization, Site Recovery Manager only applies the customization to the most recent PIT snapshot. If you recover a virtual machine with IP customization and revert to an older PIT snapshot, you must configure the IP settings manually.

Point-in-time recovery is not available with array-based replication.

Procedure

1 Configure Site Recovery Manager to retain older PIT snapshots by setting the **vrReplication > preserveMpitImagesAsSnapshots** option.

2 Use the vSphere Replication interface to configure replication of a virtual machine, selecting the option to retain a number of PIT snapshots.

3 In the Site Recovery Manager interface, add the virtual machine to a vSphere Replication protection group.

4 Include the vSphere Replication protection group in a recovery plan.

5 Run the recovery plan.

When the recovery plan is finished, the virtual machine is recovered to the recovery site, with the number of PIT snapshots that you configured.

6 In the **VMs and Templates** view, right-click the recovered virtual machine and select **Snapshot > Snapshot Manager**.

7 Select one of the PIT snapshots of this virtual machine and click **Go to**.

The recovered virtual machine reverts to the PIT snapshot that you selected.

8 (Optional) If you have configured the virtual machine for IP customization, and if you select an older PIT snapshot than the most recent one, manually configure the IP settings on the recovered virtual machine.

Cancel a Test or Recovery

You can cancel a recovery plan test whenever the status is test in progress or failover in progress.

When you cancel a test or recovery, Site Recovery Manager does not start processes, and uses certain rules to stop processes that are in progress. Canceling a failover requires you to re-run the failover.

- Processes that cannot be stopped, such as powering on or waiting for a heartbeat, run to completion before the cancellation finishes.
- Processes that add or remove storage devices are undone by cleanup operations if you cancel.

The time it takes to cancel a test or recovery depends on the type and number of processes that are currently in progress.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 Right-click the recovery plan and select **Cancel**. You can also cancel the plan from the Recovery Steps tab.

What to do next

Run a cleanup after canceling a test.

Export Recovery Plan Steps

You can export the steps of a recovery plan in various formats for future reference, or to keep a hard copy backup of your plans.

You cannot export the recovery plan steps while a test recovery or a real recovery is in progress.

Prerequisites

Verify that you have a recovery plan.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 In the **Monitor** tab, click **Recovery Steps**.

3 Click the **Export Recovery Plan Steps** icon.

You can save the recovery plan steps as HTML, XML, CSV, or MS Excel or Word document.

4 Click **Generate Report**.

5 Click **Download Report** and close the window.

View and Export a Recovery Plan History

You can view and export reports about each run of a recovery plan, test of a recovery plan, or test cleanup.

Recovery plan histories provide information about each run, test, or cleanup of a recovery plan. The history contains information about the result and the start and end times for the whole plan and for each step in the plan. You can export history at any time, but history always contains entries only for completed operations. If an operation is in progress, the history appears after the operation completes.

SRM preserves history for deleted recovery plans. You can export history reports for existing and deleted plans from **Site Recovery > Sites**. Select a site and click **Recovery Plans History** tab.

Prerequisites

You ran or tested a recovery plan, or cleaned up after a test.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 On the **Monitor** tab, click **History**.

3 (Optional) Click the Export icon for the recovery plan history for a specific time period, recovery plan run, test, or cleanup operation.

You can save the recovery plan history as HTML, XML, CSV, or MS Excel or Word document.

Delete a Recovery Plan

You can delete a recovery plan if you do not need it.

The recovery plan must be a consistent state before you can delete it.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 (Optional) On the **Monitor** tab, click **Recovery Plans History**, and click **Export History Report** to download the history of the plan.

You can view the history for deleted plans in **Recovery Plans History**.

3 Right-click the recovery plan to delete and select **Delete Recovery Plan**.

Recovery Plan Status Reference

You can monitor the status of a recovery plan and determine the operation that is allowed in each state. The state of a recovery plan is determined by the states of the protection groups within the plan.

Table 4-2. Recovery States

State	Description
Ready	Recovery steps are cleared.
Test in progress	Canceling a test moves plan to Cancel In Progress state.
Test complete	Test completed with or without errors.
Test interrupted	Server failed while a test was running.
Cleanup in progress	After successful cleanup, plan state goes to Ready. If cleanup is incomplete, state goes to Cleanup Incomplete. If you set the Force Cleanup option, state goes to Ready after an error. If a failure occurs during cleanup, state goes to Cleanup Incomplete.
Cleanup incomplete	Errors occurred during cleanup. You can run the cleanup again. When running cleanup from this state, the cleanup wizard provides an option to ignore errors.
Cleanup interrupted	Site Recovery Manager failed during cleanup. You cannot change recovery options.
Recovery in progress	If you cancel recovery, the state goes to Cancel in progress.

Table 4-2. Recovery States (Continued)

State	Description
Disaster recovery complete	During recovery at the protected site, VM shutdown enountered errors, possibly because the sites were not connected, the step before split brain. System prompt warns of split brain and to run recovery again when sites reconnect. When sites are connected, state goes to Recovery Required (split brain)
Recovery started	A recovery started on the peer site, but if the sites are not connected, the exact state is unknown. Log in to the recovery site or reconnect the sites to get the current state.
Recovery required (split brain)	Sites were disconnected during recovery. Split brain scenario detected when sites reconnect. System prompts you to run recovery again to synchronize the sites.
Recovery complete	VMs are all recovered but with errors. Running recovery again does not fix the errors. Plan goes to this state after the split brain recovery is resolved. You can see the recover steps of the last recovery run.
Incomplete recovery	Canceled recovery or datastore error. Run recovery again. You need to either resolve errors and rerun recovery, or remove protection for VMs in error. The plan detects the resolution of errors in either of these ways and updates state to Recovery Complete.
Partial recovery	Some but not all protection groups are recovered by an overlapping plan.
Recovery interrupted	A failure during recovery causes the recovery to pause. Click **Recovery** to continue. You cannot change recovery options.
Cancel in progress	Canceling a test results in Test Complete with last result canceled. Canceling a recovery results in Incomplete Recovery with last result canceled.
Reprotect in progress	If the server fails during this state, it goes to Reprotect Interrupted .
Partial reprotect	Overlapping plan was reprotected. The already reprotected groups go to Ready state, but this is valid, since the other groups are in the Recovered state.
Incomplete reprotect	Reprotect did not complete the storage operations. Sites must be connected for the reportect to succeed on the new run.
Reprotect interrupted	If the Site Recovery Manager Server fails during reprotect, run reprotect again to continue and properly clean up the state.
Waiting for user input during test	Test is paused. Dismiss the prompt to resume the test.
Waiting for user input during recovery	Recovery is paused. Dismiss the prompt to resume recovery.

Table 4-2. Recovery States (Continued)

State	Description
Protection groups in use	Plan contains groups that are being used for a test by another plan. This state also occurs when the other plan has completed a Test operation on the groups, but has not run Cleanup. Wait for the other plan to complete the test or cleanup or edit the plan to remove the groups.
Direction error	Groups are in a mixed state, which is an invalid state. Some groups are Ready in both directions: a site is protected and a site is recovered within a particular group. Remove some protection groups. For this error to occur, overlapping plans have run and reprotected all the groups in the plan already.
Plan out of sync	This state can occur under different circumstances: ■ Between a successful test recovery and a cleanup operation. You cannot edit the plan when it is in this state. Run cleanup to return the plan to the Ready state. If the plan remains in the Plan Out of Sync state, edit the plan. ■ During regular operation You can edit the plan. Opening the plan for editing causes Site Recovery Manager to force synchronization of Site Recovery Manager internal data about the plan between protection and recovery Site Recovery Manager servers, which clears the Plan Out Of Sync status .
No protection groups	The plan contains no protection groups and the plan cannot run. You can create empty plans through the API or by deleting protection groups.
Internal error	A protection group with an unknown state is in the plan, or some other unexpected error occurred. You cannot run the plan but you can delete it.

Configuring a Recovery Plan 5

You can configure a recovery plan to run commands on Site Recovery Manager Server or on a virtual machine, display messages that require a response when the plan runs, suspend non-essential virtual machines during recovery, configure dependencies between virtual machines, customize virtual machine network settings, and change the recovery priority of protected virtual machines.

A simple recovery plan that specifies only a test network to which the recovered virtual machines connect and timeout values for waiting for virtual machines to power on and be customized can provide an effective way to test a Site Recovery Manager configuration. Most recovery plans require configuration for use in production. For example, a recovery plan for an emergency at the protected site might be different from a recovery plan for the planned migration of services from one site to another.

NOTE A recovery plan always reflects the current state of the protection groups that it recovers. If any members of a protection group show a status other than OK, you must correct the problems before you can make any changes to the recovery plan.

Recovery Plan Steps

A recovery plan runs a series of steps that must be performed in a specific order for a given workflow such as a planned migration or reprotect. You cannot change the order or purpose of the steps, but you can insert your own steps that display messages and run commands.

Site Recovery Manager runs different recovery plan steps in different ways.

- Some steps run during all recoveries.
- Some steps run only during test recoveries.
- Some steps are always skipped during test recoveries.

Understanding recovery steps, their order, and the context in which they run is important when you customize a recovery plan.

Recovery Order

When you run a recovery plan, it starts by powering off the virtual machines at the protected site. Site Recovery Manager powers off virtual machines according to the priority that you set, with high-priority machines powering off last. Site Recovery Manager omits this step when you test a recovery plan.

Site Recovery Manager powers on groups of virtual machines on the recovery site according to the priority that you set. Before a priority group starts, all of the virtual machines in the next-higher priority group must recover or fail to recover. If dependencies exist between virtual machines in the same priority group, Site Recovery Manager first powers on the virtual machines on which other virtual machines depend. If Site Recovery Manager can meet the virtual machine dependencies, Site Recovery Manager attempts to power on as many virtual machines in parallel as vCenter Server supports.

Recovery Plan Timeouts and Pauses

Several types of timeouts can occur during the running of recovery plan steps. Timeouts cause the plan to pause for a specified interval to allow the step time to finish.

Message steps force the plan to pause until the user acknowledges the message. Before you add a message step to a recovery plan, make sure that it is necessary. Before you test or run a recovery plan that contains message steps, make sure that a user can monitor the progress of the plan and respond to the messages as needed.

Creating Custom Recovery Steps

You can create custom recovery steps that run commands or present messages to the user during a recovery.

Site Recovery Manager can run custom steps either on the Site Recovery Manager Server or in a virtual machine that is part of the recovery plan. You cannot run custom steps on virtual machines that are to be suspended.

During reprotect, Site Recovery Manager preserves all custom recovery steps in the recovery plan. If you perform a recovery or test after a reprotect, custom recovery steps are run on the new recovery site, which was the original protected site.

After reprotect, you can usually use custom recovery steps that show messages directly without modifications. You might need to modify some custom recovery steps after a reprotect, if these steps run commands that contain site-specific information, such as network configurations.

- Types of Custom Recovery Steps on page 57

  You can create different types of custom recovery steps to include in recovery plans.

- How Site Recovery Manager Handles Custom Recovery Step Failures on page 58

  Site Recovery Manager handles custom recovery step failures differently based on the type of recovery step.

- Create Top-Level Message Prompts or Command Steps on page 58

  You can add top-level recovery steps anywhere in the recovery plan. Top-level command steps are commands or scripts that you run on Site Recovery Manager Server during a recovery. You can also add steps that display message prompts that a user must acknowledge during a recovery.

- Create Message Prompts or Command Steps for Individual Virtual Machines on page 59

  You can create custom recovery steps to prompt users to perform tasks or for Site Recovery Manager to perform tasks on a virtual machine before or after Site Recovery Manager powers it on.

- Guidelines for Writing Command Steps on page 60

  All batch files or commands for custom recovery steps that you add to a recovery plan must meet certain requirements.

- Environment Variables for Command Steps on page 60

  Site Recovery Manager makes environment variables available that you can use in commands for custom recovery steps.

Types of Custom Recovery Steps

You can create different types of custom recovery steps to include in recovery plans.

Custom recovery steps are either command recovery steps or message prompt steps.

Command Recovery Steps

Command recovery steps contain either top-level commands or per-virtual machine commands.

Top-Level Commands	Run on the Site Recovery Manager Server. For example, you might use these commands to power on physical devices or to redirect network traffic.
Per-Virtual Machine Commands	Site Recovery Manager associates per-virtual machine commands with newly recovered virtual machines during the recovery process. You can use these commands to complete configuration tasks after powering on a virtual machine. You can run the commands either before or after powering on a virtual machine. Commands that you configure to run after the virtual machine is powered on can run either on the Site Recovery Manager Server or in the newly recovered virtual machine. Commands that run on the newly recovered virtual machine are run in the context of the user account that VMware Tools uses on the recovered virtual machine. Depending on the function of the command that you write, you might need to change the user account that VMware Tools uses on the recovered virtual machine.

Message Prompt Recovery Steps

Present a message in the Site Recovery Manager user interface during the recovery. You can use this message to pause the recovery and provide information to the user running the recovery plan. For example, the message can instruct users to perform a manual recovery task or to verify steps. The only action users can take in direct response to a prompt is to dismiss the message, which allows the recovery to continue.

How Site Recovery Manager Handles Custom Recovery Step Failures

Site Recovery Manager handles custom recovery step failures differently based on the type of recovery step.

Site Recovery Manager attempts to complete all custom recovery steps, but some command recovery steps might fail to finish.

Command Recovery Steps

By default, Site Recovery Manager waits for 5 minutes for command recovery steps to finish. You can configure the timeout for each command. If a command finishes within this timeout period, the next recovery step in the recovery plan runs. How Site Recovery Manager handles failures of custom commands depends on the type of command.

Type of Command	Description
Top-level commands	If a recovery step fails, Site Recovery Manager logs the failure and shows a warning on the **Recovery Steps** tab. Subsequent custom recovery steps continue to run.
Per-virtual machine commands	Run in batches either before or after a virtual machine powers on. If a command fails, the remaining per-virtual machine commands in the batch do not run. For example, if you add five commands to run before power on and five commands to run after power on, and the third command in the batch before power on fails, the remaining two commands to run before power on do not run. Site Recovery Manager does not power on the virtual machine and so cannot run any post-power on commands.

Message Prompt Recovery Steps

Custom recovery steps that issue a message prompt cannot fail. The recovery plan pauses until the user dismisses the prompt.

Create Top-Level Message Prompts or Command Steps

You can add top-level recovery steps anywhere in the recovery plan. Top-level command steps are commands or scripts that you run on Site Recovery Manager Server during a recovery. You can also add steps that display message prompts that a user must acknowledge during a recovery.

Prerequisites

- You have a recovery plan to which to add custom steps.
- For information about writing the commands to add to command steps, see "Guidelines for Writing Command Steps," on page 60 and "Environment Variables for Command Steps," on page 60.

Procedure

1. In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.
2. On the **Monitor** tab, click **Recovery Steps**.
3. Use the **View** drop-down menu to select the type of recovery plan run to which to add a step.

Option	Description
Test Steps	Add a step to run when you test a recovery plan.
Recovery Steps	Add a step to run when you perform planned migration or disaster recovery

   You cannot add steps in the cleanup or reprotect operations.

4. Right-click a step before or after which to add a custom step, and select **Add Step**.

5 Select **Command on SRM Server** or **Prompt**.

6 In the **Name** text box, enter a name for the step.

The step name appears in the list of steps in the **Recovery Steps** view.

7 In the **Content** text box, enter the commands for the step to run.

- If you selected **Command on SRM Server**, enter the command or script to run.
- If you selected **Prompt**, enter the text of the message to display during the recovery plan run.

8 (Optional) Modify the **Timeout** setting for the command to run on Site Recovery Manager Server.

This option is not available if you create a prompt step.

9 Select where in the sequence of steps to insert the new step.

- **Before selected step**
- **After selected step**

10 Click **OK** to add the step to the recovery plan.

Create Message Prompts or Command Steps for Individual Virtual Machines

You can create custom recovery steps to prompt users to perform tasks or for Site Recovery Manager to perform tasks on a virtual machine before or after Site Recovery Manager powers it on.

Site Recovery Manager associates command steps with a protected or recovered virtual machine in the same way as customization information. If multiple recovery plans contain the same virtual machine, Site Recovery Manager includes the commands and prompts in all of the recovery plans .

Prerequisites

- You have a recovery plan to which to add custom steps.
- For information about writing the commands to add to command steps, see "Guidelines for Writing Command Steps," on page 60 and "Environment Variables for Command Steps," on page 60.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 On the **Related Objects** tab, click **Virtual Machines**.

3 Right-click a virtual machine and click **Configure Recovery**.

4 On the **Recovery Properties** tab, click **Pre-Power On Steps** or **Post-Power On Steps**.

5 Click the plus icon to add a step.

6 Select the type of step to create.

Option	Description
Prompt	Prompts users to perform a task or to provide information that the user must acknowledge before the plan continues to the next step. This option is available for both pre-power on steps and post-power on steps.
Command on SRM Server	Runs a command on Site Recovery Manager Server. This option is available for both pre-power on steps and post-power on steps.
Command on Recovered VM	Runs a command on the recovered virtual machine. This option is only available for post-power on steps.

7 In the **Name** text box, enter a name for the step.

The step name appears in the list of steps in the **Recovery Steps** view.

8 In the **Content** text box, enter the commands for the step to run.

- If you selected **Command on SRM Server** or **Command on Recovered VM**, enter the command or script to run.
- If you selected **Prompt**, enter the text of the message to display during the recovery plan run.

9 (Optional) Modify the **Timeout** setting for the command to run on Site Recovery Manager Server.

This option is not available if you create a prompt step.

10 Click **OK** to add the step to the recovery plan.

11 Click **OK** to reconfigure the virtual machine to run the command before or after it powers on.

Guidelines for Writing Command Steps

All batch files or commands for custom recovery steps that you add to a recovery plan must meet certain requirements.

When you create a command step to add to a recovery plan, make sure that it takes into account the environment in which it must run. Errors in a command step affect the integrity of a recovery plan. Test the command on Site Recovery Manager Server on the recovery site before you add it to the plan.

- You must start the Windows command shell using its full path on the local host. For example, to run a script located in `c:\alarmscript.bat`, use the following command line:

  ```
  c:\windows\system32\cmd.exe /c c:\alarmscript.bat
  ```

- You must install batch files and commands on the Site Recovery Manager Server at the recovery site.
- Batch files and commands must finish within 300 seconds. Otherwise, the recovery plan terminates with an error. To change this limit, see "Change Recovery Settings," on page 105.
- Batch files or commands that produce output that contains characters with ASCII values greater than 127 must use UTF-8 encoding. Site Recovery Manager records only the final 4KB of script output in log files and in the recovery history. Scripts that produce more output should redirect the output to a file rather than sending it to the standard output to be logged.

Environment Variables for Command Steps

Site Recovery Manager makes environment variables available that you can use in commands for custom recovery steps.

Command steps run with the identity of the LocalSystem account on the Site Recovery Manager Server host at the recovery site. When a command step runs, Site Recovery Manager makes environment variables available for it to use.

Table 5-1. Environment Variables Available to All Command Steps

Name	Value	Example
VMware_RecoveryName	Name of the recovery plan that is running.	Plan A
VMware_RecoveryMode	Recovery mode.	Test or recovery
VMware_VC_Host	Host name of the vCenter Server at the recovery site.	vc_hostname.example.com
VMware_VC_Port	Network port used to contact vCenter Server.	443

Site Recovery Manager makes additional environment variables available for per-virtual machine command steps that run either on Site Recovery Manager Server or on the recovered virtual machine.

Table 5-2. Environment Variables Available to Per-Virtual Machine Command Steps

Name	Value	Example
VMware_VM_Uuid	UUID used by vCenter to uniquely identify this virtual machine.	4212145a-eeae-a02c-e525-ebba70b0d4f3
VMware_VM_Name	Name of this virtual machine, as set at the protected site.	My New Virtual Machine
VMware_VM_Ref	Managed object ID of the virtual machine.	vm-1199
*VMware_VM_Guest*Name	Name of the guest OS as defined by the VIM API.	otherGuest
*VMware_VM_Guest*Ip	IP address of the virtual machine, if known.	192.168.0.103
VMware_VM_Path	Path to this VMDK of this virtual machine.	`[datastore-123] jquser-vm2/jquser-vm2.vmdk`

Suspend Virtual Machines When a Recovery Plan Runs

Site Recovery Manager can suspend virtual machines on the recovery site during a recovery and a test recovery.

Suspending virtual machines on the recovery site is useful in active-active datacenter environments and where non-critical workloads run on recovery sites. By suspending any virtual machines that host non-critical workloads on the recovery site, Site Recovery Manager frees capacity for the recovered virtual machines. Site Recovery Manager resumes virtual machines that are suspended during a failover operation when the failover runs in the opposite direction.

You can only add virtual machines to suspend at the recovery site.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 In the **Monitor** tab, click **Recovery Steps**.

3 Right-click **Suspend Non-critical VMs at Recovery Site** and select **Add Non-Critical VM**.

4 Select virtual machines on the recovery site to suspend during a recovery.

5 Click **OK**.

Site Recovery Manager suspends the virtual machines on the recovery site when the recovery plan runs.

Specify the Recovery Priority of a Virtual Machine

By default, Site Recovery Manager sets all virtual machines in a new recovery plan to recovery priority level 3. You can increase or decrease the recovery priority of a virtual machine. The recovery priority specifies the shutdown and power on order of virtual machines.

If you change the priority of a virtual machine, Site Recovery Manager applies the new priority to all recovery plans that contain this virtual machine.

Site Recovery Manager starts virtual machines on the recovery site according to the priority that you set. Site Recovery Manager starts priority 1 virtual machines first, then priority 2 virtual machines second, and so on. Site Recovery Manager uses VMware Tools heartbeat to discover when a virtual machine is running on the recovery site. In this way, Site Recovery Manager can ensure that all virtual machines of a given priority are running before it starts the virtual machines of the next priority. For this reason, you must install VMware Tools on protected virtual machines.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 On the **Related Objects** tab, click **Virtual Machines**.

3 Right-click a virtual machine and select **All Priority Actions**.

4 Select a new priority for the virtual machine.

The highest priority is 1. The lowest priority is 5.

5 Click **Yes** to confirm the change of priority.

Configure Virtual Machine Dependencies

If a virtual machine depends on services that run on another virtual machine in the same protection group, you can configure a dependency between the virtual machines. By configuring a dependency, you can ensure that the virtual machines start on the recovery site in the correct order. Dependencies are only valid if the virtual machines have the same priority.

When a recovery plan runs, Site Recovery Manager starts the virtual machines that other virtual machines depend on before it starts the virtual machines with the dependencies. If Site Recovery Manager cannot start a virtual machine that another virtual machine depends on, the recovery plan continues with a warning. You can only configure dependencies between virtual machines that are in the same recovery priority group. If you configure a virtual machine to be dependent on a virtual machine that is in a lower priority group, Site Recovery Manager overrides the dependency and first starts the virtual machine that is in the higher priority group.

If you remove a protection group that contains the dependent virtual machine from the recovery plan the status of the protection group is set to `Not in this Plan` in the dependencies for the virtual machine with the dependency. If the configured virtual machine has a different priority than the virtual machine that it depends on, the status of the dependent virtual machine is set to Lower Priority or Higher Priority.

Prerequisites

- Verify that the virtual machine with the dependency and the virtual machine that it depends on are in the same recovery plan.
- Verify that the virtual machine with the dependency and the virtual machine that it depends on are in the same recovery priority group.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 On the **Related Objects** tab, click **Virtual Machines**.

3 Right-click a virtual machine that depends on one or more other virtual machines and select **Configure Recovery**.

4 Expand **VM Dependencies**.

5 Verify the virtual machines that this virtual machine depends on are on and verify the status of the dependencies is OK.

6 (Optional) To remove a dependency, select a virtual machine from the list of virtual machines that this virtual machine depends on and click **Remove**.

7 Click **OK**.

Configure Virtual Machine Startup and Shutdown Options

You can configure how a virtual machine starts up and shuts down on the recovery site during a recovery.

You can configure whether to shut down the guest operating system of a virtual machine before it powers off on the protected site. You can configure whether to power on a virtual machine on the recovery site. You can also configure delays after powering on a virtual machine to allow VMware Tools or other applications to start on the recovered virtual machine before the recovery plan continues.

Prerequisites

You created a recovery plan.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 On the **Related Objects** tab, click **Virtual Machines**.

3 Right-click a virtual machine and select **Configure Recovery**.

4 Expand **Shutdown Action** and select the shutdown method for this virtual machine.

Option	Description
Shutdown guest OS before power off	Gracefully shuts down the virtual machine before powering it off. You can set a timeout period for the shutdown operation. Setting the timeout period to 0 is equivalent to the Power off option. This option requires that VMware Tools are running on the virtual machine.
Power off	Powers off the virtual machine without shutting down the guest operating system.

5 Expand **Startup Action** and select whether to power on the virtual machine after a recovery.

Option	Description
Power on	Powers on the virtual machine on the recovery site.
Do not power on	Recovers the virtual machine but does not power it on.

6 (Optional) Select or deselect the **Wait for VMware tools** check box.

This option is only available if you selected **Power on** in Step 5.

If you select **Wait for VMware tools**, Site Recovery Manager waits until VMware Tools starts after powering on the virtual machine before the recovery plan continues to the next step. You can set a timeout period for VMware Tools to start.

7 (Optional) Select or deselect the **Additional Delay before running Post Power On steps and starting dependent VMs** check box and specify the time for the additional delay.

This option is only available if you selected **Power on** in Step 5.

For example, you might specify an additional delay after powering on a virtual machine to allow applications to start up that another virtual machine depends on.

Customizing IP Properties for Virtual Machines

6

You can customize IP settings for virtual machines for the protected site and the recovery site. Customizing the IP properties of a virtual machine overrides the default IP settings when the recovered virtual machine starts at the destination site.

If you do not customize the IP properties of a virtual machine, Site Recovery Manager uses the IP settings for the recovery site during a recovery or a test from the protection site to the recovery site.
Site Recovery Manager uses the IP settings for the protection site after reprotect during the recovery or a test from the original recovery site to the original protection site.

Site Recovery Manager supports different types of IP customization.

- Use IPv4 and IPv6 addresses.
- Configure different IP customizations for each site.
- Use DHCP, Static IPv4, or Static IPv6 addresses.
- Customize addresses of Windows and Linux virtual machines.
- Customize multiple NICs for each virtual machine.

For the list of guest operating systems for which Site Recovery Manager supports IP customization, see the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.

You associate customization settings with protected virtual machines. As a result, if the same protected virtual machine is a part of multiple recovery plans, then all recovery plans use a single copy of the customization settings. You configure IP customization as part of the process of configuring the recovery properties of a virtual machine.

If you do not customize a NIC on the recovery site, the NIC continues to use the IP settings from the protected site, and vice versa, and Site Recovery Manager does not apply IP customization to the virtual machine during recovery.

You can apply IP customizations to individual or to multiple virtual machines.

If you configure IP customization on virtual machines, Site Recovery Manager adds recovery steps to those virtual machines.

Guest OS Startup	The Guest Startup process happens in parallel for all virtual machines for which you configure IP customization.
Customize IP	Site Recovery Manager pushes the IP customizations to the virtual machine.
Guest OS Shutdown	Site Recovery Manager shuts down the virtual machine and reboots it to ensure that the changes take effect and that the guest operating system services apply them when the virtual machine restarts.

After the IP customization process finishes, virtual machines power on according to the priority groups and any dependencies that you set. The power on process happens immediately before the Wait for VMTools process for each virtual machine.

NOTE To customize the IP properties of a virtual machine, you must install VMware Tools or the VMware Operating System Specific Packages (OSP) on the virtual machine. See http://www.vmware.com/download/packages.html.

- Manually Customize IP Properties For an Individual Virtual Machine on page 66

  You can customize IP settings manually for individual virtual machines for both the protected site and the recovery site.

- Customizing IP Properties for Multiple Virtual Machines on page 67

  You can customize the IP properties for multiple virtual machines on the protected and recovery sites by using the DR IP Customizer tool and by defining subnet-level IP mapping rules.

Manually Customize IP Properties For an Individual Virtual Machine

You can customize IP settings manually for individual virtual machines for both the protected site and the recovery site.

NOTE Virtual machines with manually defined IP customization are not subject to the IP Mapping Rule evaluation during recovery. Manually-specified IP configuration takes precedence over IP mapping rules.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**, and select a recovery plan.

2 On the **Related Objects** tab, click **Virtual Machines**.

3 Right-click a virtual machine and click **Configure Recovery**.

4 Click the **IP Customization** tab and select **Manual IP customization**.

5 Select the NIC for which you want to modify IP Settings.

6 Click **Configure Protection** or **Configure Recovery**, depending on whether you want to configure IP settings on the protected site or on the recovery site.

7 Click the **General** tab to configure settings.

   a Choose the type of addressing to be used.

     Available options include DHCP, static IPv4, or static IPv6.

   b For static addresses, enter an IP address, subnet information, and gateway server addresses.

     Alternately, if the virtual machine is powered on and has VMware Tools installed, you can click **Retrieve** to import current settings configured on the virtual machine.

8 Click the **DNS** tab to configure DNS settings.

   a Choose how DNS servers are found.

     You can use DHCP to find DNS servers or you can specify primary and alternate DNS servers.

   b Enter a DNS suffix and click **Add** or select an existing DNS suffix and click **Remove**, **Move Up**, or **Move Down**.

9 Click the **WINS** tab to enter primary and secondary WINS addresses.

   The **WINS** tab is available only when configuring DHCP or IPv4 addresses for Windows virtual machines.

10 Repeat Step 6 through Step 9 to configure recovery site or protected site settings, if required.

   For example, if you configured IP settings for the protected site, you might want to configure settings for the recovery site.

11 Repeat the configuration process for other NICs, as required.

Customizing IP Properties for Multiple Virtual Machines

You can customize the IP properties for multiple virtual machines on the protected and recovery sites by using the DR IP Customizer tool and by defining subnet-level IP mapping rules.

In previous releases of Site Recovery Manager, you customized IP properties for multiple virtual machines by using the DR IP Customizer tool. In addition to DR IP Customizer, with Site Recovery Manager 5.8 you can customize IP properties for multiple virtual machines by defining subnet-level IP customization rules.

You can use subnet-level IP customization rules in combination with DR IP Customizer.

- Using DR IP Customizer is a fast way to define explicit IP customization settings for multiple virtual machines by using a CSV file.
- You apply subnet-level IP customization rules to virtual machines by using the vSphere Web Client.

Virtual machines that you configure by using DR IP Customizer are not subject to subnet-level IP customization rules. You can achieve the same IP customization results by using either DR IP Customizer or IP subnet rules. In Site Recovery Manager 5.8, the DR IP Customizer provides more control over IP configuration of individual virtual machines, such as customizing static IPv6. This control is useful when you upgrade from an earlier version of Site Recovery Manager in which you used DR IP Customizer.

Customizing IP Properties for Multiple Virtual Machines By Using the DR IP Customizer Tool

The DR IP Customizer tool allows you to define explicit IP customization settings for multiple protected virtual machines on the protected and recovery sites.

In addition to defining subnet IP mapping rules, you can use the DR IP Customizer tool to apply customized networking settings to virtual machines when they start on the recovery site. You provide the customized IP settings to the DR IP Customizer tool in a comma-separated value (CSV) file.

Rather than manually creating a CSV file, you can use the DR IP Customizer tool to export a CSV file that contains information about the networking configurations of the protected virtual machines. You can use this file as a template for the CSV file to apply on the recovery site by customizing the values in the file.

1 Run DR IP Customizer to generate a CSV file that contains the networking information for the protected virtual machines.

2 Modify the generated CSV file with networking information that is relevant to the recovery site.

3 Run DR IP Customizer again to apply the CSV with the modified networking configurations to apply when the virtual machines start up on the recovery site.

You can run the DR IP Customizer tool on either the protected site or on the recovery site. Virtual machine IDs for protected virtual machines are different at each site, so whichever site you use when you run the DR IP Customizer tool to generate the CSV file, you must use the same site when you run DR IP Customizer again to apply the settings.

You can customize the IP settings for the protected and the recovery sites so that Site Recovery Manager uses the correct configurations during reprotect operations.

For the list of guest operating systems for which Site Recovery Manager supports IP customization, see the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.

Report IP Address Mappings for Recovery Plans

The IP address map reporter generates an XML document describing the IP properties of protected virtual machines and their placeholders, grouped by site and recovery plan. This information can help you understand the network requirements of a recovery plan.

Because the IP address mapping reporter must connect to both sites, you can run the command at either site. You are prompted to supply the vCenter login credentials for each site when the command runs.

Procedure

1 Open a command shell on the Site Recovery Manager Server host at either the protected or recovery site.

2 Change to the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin` directory.

3 Run the `dr-ip-reporter.exe` command, as shown in this example.

```
dr-ip-reporter.exe
--cfg ..\config\vmware-dr.xml
--out path_to_report_file.xml
--vc vcenter_server_address
```

To restrict the list of networks to just the ones required by a specific recovery plan, include the `-plan` option on the command line, as shown in this example.

```
dr-ip-reporter.exe
--cfg ..\config\vmware-dr.xml
--out path_to_report_file.xml
--vc vcenter_server_address
--plan recovery_plan_name
```

NOTE The command normally asks you to verify the thumbprints presented by the certificates at each site. You can suppress the verification request by including the `-I` option.

Syntax of the DR IP Customizer Tool

The DR IP Customizer tool includes options that you can use to gather networking information about the virtual machines that Site Recovery Manager protects. You can also use the options to apply customizations to virtual machines when they start up on the recovery site.

NOTE This release of Site Recovery Manager allows you to define subnet-level IP mapping rules to customize IP settings on virtual machines, as well as by using the DR IP Customizer tool. You can use subnet-level IP mapping rules in combination with DR IP Customizer. For information about how you can use subnet-level IP mapping rules and DR IP Customizer together, see "Customizing IP Properties for Multiple Virtual Machines," on page 67.

You find the `dr-ip-customizer.exe` executable file in `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin` on the Site Recovery Manager Server host machine. When you run `dr-ip-customizer.exe`, you specify different options depending on whether you are generating or applying a comma-separated value (CSV) file.

```
dr-ip-customizer.exe
--cfg SRM Server configuration XML
--cmd apply/drop/generate
[--csv Name of existing CSV File]
[--out Name of new CSV file to generate]
[--vc vCenter Server address]
[--ignore-thumbprint]
[--extra-dns-columns]
[--verbose]
```

You can run the DR IP Customizer tool on either the protected site or on the recovery site. Virtual machine IDs for protected virtual machines are different at each site, so whichever site you use when you run the DR IP Customizer tool to generate the CSV file, you must use the same site when you run DR IP Customizer again to apply the settings.

Some of the options that the DR IP Customizer tool provides are mandatory, others are optional.

Table 6-1. DR IP Customizer Options

Option	Description	Mandatory
`-h [ --help ]`	Displays usage information about `dr-ip-customizer.exe`.	No
`--cfg arg`	Path to the XML configuration file of the Site Recovery Manager Server, `vmware-dr.xml` file.	Yes

Table 6-1. DR IP Customizer Options (Continued)

Option	Description	Mandatory
`--cmd arg`	You specify different commands to run DR IP Customizer in different modes. ■ The `apply` command applies the network customization settings from an existing CSV file to the recovery plans on the Site Recovery Manager Server instances. ■ The `generate` command generates a basic CSV file for all virtual machines that Site Recovery Manager protects for a vCenter Server instance. ■ The `drop` command removes the recovery settings from virtual machines specified by the input CSV file. Always provide the same vCenter Server instance for the `apply` and `drop` commands as the one that you used to generate the CSV file.	Yes
`--csv arg`	Path to the CSV file to use as input.	Yes, when running the `apply` and `drop` commands.
`-o [ --out ] arg`	Name of the new CSV output file that the `generate` command creates. If you provide the name of an existing CSV file, the `generate` command overwrites its current contents.	Yes, when you run the `generate` command.
`--vc arg`	vCenter Server address. Virtual machine IDs for the protected virtual machines are different at each site. Use the same vCenter Server instance when you generate the CSV file and when you apply it.	Yes
`-i [ --ignore-thumbprint ]`	Ignore the vCenter Server thumbprint confirmation prompt.	No
`-e [ --extra-dns-columns ]`	Obsolete.	No
`-v [ --verbose ]`	Enable verbose output. You can include a `--verbose` option on any `dr-ip-customizer.exe` command line to log additional diagnostic messages.	No

Structure of the DR IP Customizer CSV File

The DR IP Customizer comma-separated value (CSV) file consists of a header row that defines the meaning of each column in the file, and one or more rows for each placeholder virtual machine in a recovery plan.

Note This release of Site Recovery Manager allows you to define subnet-level IP mapping rules to customize IP settings on virtual machines, as well as by using the DR IP Customizer tool. You can use subnet-level IP mapping rules in combination with DR IP Customizer. For information about how you can use subnet-level IP mapping rules and DR IP Customizer together, see "Customizing IP Properties for Multiple Virtual Machines," on page 67.

Configuring IP settings for both sites is optional. You can provide settings for only the protected site, or settings for only the recovery site, or settings for both sites. You can configure each site to use a different set of network adapters in a completely different way.

Certain fields in the CSV file must be completed for every row. Other fields can be left blank if no customized setting is required.

Table 6-2. Columns of the DR IP Customizer CSV File

Column	Description	Customization Rules
VM ID	Unique identifier that DR IP Customizer uses to collect information from multiple rows for application to a single virtual machine. This ID is internal to DR IP Customizer and is not the same as the virtual machine ID that vCenter Server uses.	Not customizable. Cannot be blank.
VM Name	The human-readable name of the virtual machine as it appears in the vCenter Server inventory.	Not customizable. Cannot be blank.
vCenter Server	Address of a vCenter Server instance on either the protected site or the recovery site. You set the IP settings for a virtual machine on each site in the vCenter Server column.	Not customizable. Cannot be blank. This column can contain both vCenter Server instances. Each vCenter Server instance requires its own row. You can configure one set of IP settings to use on one site and another set of IP settings to use on the other site. You can also provide IP settings to be used on both sites, for reprotect operations.
Adapter ID	ID of the adapter to customize. Adapter ID 0 sets global settings on all adapters for a virtual machine. Setting values on Adapter ID 1, 2, 3, and so on, configures settings for specific NICs on a virtual machine.	Customizable. Cannot be left blank. The only fields that you can modify for a row in which the Adapter ID is 0 are DNS Server(s) and DNS Suffix(es). These values, if specified, are inherited by all other adapters in use by that VM ID. You can include multiple DNS servers on multiple lines in the CSV file. For example, if you require two global DNS hosts, you include two lines for Adapter ID 0. ■ One line that contains all the virtual machine information plus one DNS host. ■ One line that contains only the second DNS host. To add another DNS server to a specific adapter, add the DNS server to the appropriate Adapter line. For example, add the DNS server to Adapter ID 1.
DNS Domain	DNS domain for this adapter.	Customizable. Can be left blank. If you do enter a value, it must be in the format **`example.company.com`**.

Table 6-2. Columns of the DR IP Customizer CSV File (Continued)

Column	Description	Customization Rules
Net BIOS	Select whether to activate NetBIOS on this adapter.	Customizable. Can be left blank. If not left empty, this column must contain one of the following strings: `disableNetBIOS`, `enableNetBIOS`, or `enableNetBIOSViaDhcp`.
Primary WINS	DR IP Customizer validates that WINS settings are applied only to Windows virtual machines, but it does not validate NetBIOS settings.	Customizable. Can be left blank.
Secondary WINS	DR IP Customizer validates that WINS settings are applied only to Windows virtual machines, but it does not validate NetBIOS settings.	Customizable. Can be left blank.
IP Address	IPv4 address for this virtual machine.	Customizable. Cannot be blank. Virtual machines can have multiple virtual network adapters. You can configure each virtual network adapter with one static IPv4 address or one static IPv6 address. For example, if you set a static address for IPv4, you must set the IPv6 address to DHCP.
Subnet Mask	Subnet mask for this virtual machine.	Customizable. Can be left blank.
Gateway(s)	IPv4 gateway or gateways for this virtual machine.	Customizable. Can be left blank.
IPv6 Address	IPv6 address for this virtual machine.	Customizable. Can be left blank if you do not use IPv6. Virtual machines can have multiple virtual network adapters. You can configure each virtual network adapter with one static IPv4 address or one static IPv6 address. For example, if you set a static address for IPv6, you must set the IPv4 address to DHCP. If you run Site Recovery Manager Server on Windows Server 2003 and you customize IPv6 addresses for a virtual machine, you must enable IPv6 on the Site Recovery Manager Server instances. Site Recovery Manager performs validation of IP addresses during customization, which requires IPv6 to be enabled on the Site Recovery Manager Server if you are customizing IPv6 addresses. Later versions of Windows Server have IPv6 enabled by default.
IPv6 Subnet Prefix length	Ipv6 subnet prefix length to use.	Customizable. Can be left blank.
IPv6 Gateway(s)	IPv4 gateway or gateways for this adapter.	Customizable. Can be left blank.

Table 6-2. Columns of the DR IP Customizer CSV File (Continued)

Column	Description	Customization Rules
DNS Server(s)	Address of the DNS server or servers.	Customizable. Can be left blank. If you enter this setting in an Adapter ID 0 row, it is treated as a global setting. On Windows virtual machines, this setting applies for each adapter if you set it in the Adapter ID rows other than Adapter ID 0. On Linux virtual machines, this is always a global setting for all adapters. This column can contain one or more IPv4 or IPv6 DNS servers for each NIC.
DNS Suffix(es)	Suffix or suffixes for DNS servers.	Customizable. Can be left blank. These are global settings for all adapters on both Windows and Linux virtual machines.

Modifying the DR IP Customizer CSV File

You modify the DR IP Customizer comma-separated value (CSV) file to apply customized networking settings to virtual machines when they start on the recovery site.

NOTE This release of Site Recovery Manager allows you to define subnet-level IP mapping rules to customize IP settings on virtual machines, as well as by using the DR IP Customizer tool. You can use subnet-level IP mapping rules in combination with DR IP Customizer. For information about how you can use subnet-level IP mapping rules and DR IP Customizer together, see "Customizing IP Properties for Multiple Virtual Machines," on page 67.

One challenge of representing virtual machine network configurations in a CSV file is that virtual machine configurations include hierarchical information. For example, a single virtual machine might contain multiple adapters, and each adapter might have multiple listings for elements such as gateways. The CSV format does not provide a system for hierarchical representations. As a result, each row in the CSV file that the DR IP Customizer generates might provide some or all of the information for a specific virtual machine.

For a virtual machine with a simple network configuration, all the information can be included in a single row. In the case of a more complicated virtual machine, multiple rows might be required. Virtual machines with multiple network cards or multiple gateways require multiple rows. Each row in the CSV file includes identification information that describes to which virtual machine and adapter the information applies. Information is aggregated to be applied to the appropriate virtual machine.

Follow these guidelines when you modify the DR IP Customizer CSV file.

- Omit values if a setting is not required.
- Use the minimum number of rows possible for each adapter.
- Do not use commas in any field.
- Specify Adapter ID settings as needed. DR IP Customizer applies settings that you specify on Adapter ID 0 to all NICs. To apply settings to individual NICs, specify the values in the Adapter ID 1, 2, ..., *n* fields.
- To specify more than one value for a column, create an additional row for that adapter and include the value in the column in that row. To ensure that the additional row is associated with the intended virtual machine, copy the VM ID, VM Name, vCenter Server, and Adapter ID column values.

- To specify an IP address for a network adapter on each of the protected and recovery sites, or to specify multiple DNS server addresses, add a new row for each address. Copy the VM ID, VM Name, and Adapter ID values to each row.

Examples of DR IP Customizer CSV Files

You obtain a CSV file that contains the networking information for the protected virtual machines on the vCenter Server by running `dr-ip-customizer.exe` with the `--cmd generate` command. You edit the CSV file to customize the IP settings of the protected virtual machines.

You can download a bundle of the example CSV files that this section describes.

NOTE This release of Site Recovery Manager allows you to define subnet-level IP mapping rules to customize IP settings on virtual machines, as well as by using the DR IP Customizer tool. You can use subnet-level IP mapping rules in combination with DR IP Customizer. For information about how you can use subnet-level IP mapping rules and DR IP Customizer together, see "Customizing IP Properties for Multiple Virtual Machines," on page 67.

Example: A Generated DR IP Customizer CSV File

For a simple setup with only two protected virtual machines, the generated CSV file might contain only the virtual machine ID, the virtual machine name, the names of the vCenter Server instances on both sites, and a single adapter.

```
VM ID,VM Name,vCenter Server,Adapter ID,DNS Domain,Net BIOS,
Primary WINS,Secondary WINS,IP Address,Subnet Mask,Gateway(s),
IPv6 Address,IPv6 Subnet Prefix length,IPv6 Gateway(s),
DNS Server(s),DNS Suffix(es)
protected-vm-10301,vm-3-win,vcenter-server-site-B,0,,,,,,,,,,,
protected-vm-10301,vm-3-win,vcenter-server-site-A,0,,,,,,,,,,,
protected-vm-20175,vm-1-linux,vcenter-server-site-B,0,,,,,,,,,,,
protected-vm-20175,vm-1-linux,vcenter-server-site-A,0,,,,,,,,,,,
```

This generated CSV file shows two virtual machines, vm-3-win and vm-1-linux. The virtual machines are present on the protected site and on the recovery site, vcenter-server-site-B, and vcenter-server-site-A. DR IP Customizer generates an entry for each virtual machine and each site with Adapter ID 0. You can add additional lines to customize each NIC, once you are aware of how many NICs are on each virtual machine.

Example: Setting Static IPv4 Addresses

You can modify the generated CSV file to assign two network adapters with static IPv4 addresses to one of the virtual machines, vm-3-win, on the protected site and the recovery site.

For readability, the example CSV file in the following table omits empty columns. The DNS Domain, NetBIOS, IPv6 Address, IPv6 Subnet Prefix length, and IPv6 Gateway(s) columns are all omitted.

Table 6-3. Setting Static IPv4 Addresses in a Modified CSV File

VM ID	VM Name	vCenter Server	Adapter ID	Primary WINS	Secondary WINS	IP Address	Subnet Mask	Gateway(s)	DNS Server(s)	DNS Suffix(es)
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							eng.example.com

Table 6-3. Setting Static IPv4 Addresses in a Modified CSV File (Continued)

VM ID	VM Name	vCenter Server	Adapter ID	Primary WINS	Secondary WINS	IP Address	Subnet Mask	Gateway(s)	DNS Server(s)	DNS Suffix(es)
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.255.0	192.168.1.1	1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
protected-vm-10301		vcenter-server-site-A	1			192.168.0.21	255.255.255.0	192.168.0.1		
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

The information in this CSV file applies different static IPv4 settings to vm-3-win on the protected site and on the recovery site.

- On the vcenter-server-site-B site:
  - Sets the DNS suffixes example.com and eng.example.com for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, a static IPv4 address 192.168.1.21, and DNS server 1.1.1.1.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, a static IPv4 address 192.168.1.22, and DNS server 1.1.1.2.
- On the vcenter-server-site-A site:
  - Sets the DNS suffixes example.com and eng.example.com for all NICs for this virtual machine.
  - Sets the DNS servers 1.1.0.1 and 1.1.0.2 for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, with a static IPv4 address 192.168.0.21.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 1.2.3.4 and 1.2.3.5 and a static IPv4 address 192.168.0.22.

Example: Setting Static and DHCP IPv4 Addresses

You can modify the generated CSV file to assign multiple NICs to one of the virtual machines, vm-3-win, that use a combination of static and DHCP IPv4 addresses. The settings can be different on the protected site and the recovery site.

For readability, the example CSV file in the following table omits empty columns. The DNS Domain, NetBIOS, IPv6 Address, IPv6 Subnet Prefix length, and IPv6 Gateway(s) columns are all omitted.

Table 6-4. Setting Static and DHCP IPv4 Addresses in a Modified CSV File

VM ID	VM Name	vCenter Server	Adapter ID	Primary WINS	Secondary WINS	IP Address	Subnet Mask	Gateway(s)	DNS Server(s)	DNS Suffix(es)
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	dhcp			1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
protected-vm-10301		vcenter-server-site-A	1			dhcp				
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

The information in this CSV file applies different static and dynamic IPv4 settings to vm-3-win on the protected site and on the recovery site.

- On site vcenter-server-site-B:
  - Sets the DNS suffixes example.com and eng.example.com for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, that uses DHCP to obtain an IP address and sets the static DNS server 1.1.1.1.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, with a static IPv4 address 192.168.1.22 and DNS server 1.1.1.2.
- On site vcenter-server-site-A:
  - Sets the DNS suffixes to example.com and eng.example.com for all NICs for this virtual machine.
  - Sets the DNS servers 1.1.0.1 and 1.1.0.2 for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, that uses DHCP to obtain an IPv4 address and the globally assigned DNS server information.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 1.2.3.4 and 1.2.3.5, and a static IPv4 address 192.168.0.22.

Example: Setting Static and DHCP IPv4 and IPv6 Addresses

You can modify the generated CSV file to assign multiple NICs to vm-3-win, one of the virtual machines. The NICs can use a combination of static and DHCP IPv4 and IPv6 addresses. The settings can be different on both the protected site and the recovery site.

For readability, the example CSV file in the following table omits empty columns. The DNS Domain and NetBIOS columns are omitted.

Table 6-5. Setting Static and DHCP IPv4 and IPv6 Addresses in a Modified CSV File

VM ID	VM Name	vCenter Server	Adapter ID	Primary WINS	Secondary WINS	IP Address	Subnet Mask	Gateway(s)	IPv6 Address	IPv6 Subnet Prefix length	IPv6 Gateway(s)	DNS Server(s)	DNS Suffix(es)
protected-vm-10301	vm-3-win	vcenter-server-site-B	0										example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0										eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.255.0	192.168.1.1	dhcp			1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	dhcp			::ffff:192.168.1.22	32	::ffff:192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0										example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0										eng.example.com
protected-vm-10301		vcenter-server-site-A	1			dhcp			::ffff:192.168.0.22	32	::ffff:192.168.0.1	::ffff:192.168.0.250	

Table 6-5. Setting Static and DHCP IPv4 and IPv6 Addresses in a Modified CSV File (Continued)

VM ID	VM Name	vCenter Server	Adapter ID	Primary WINS	Secondary WINS	IP Address	Subnet Mask	Gateway(s)	IPv6 Address	IPv6 Subnet Prefix length	IPv6 Gateway(s)	DNS Server(s)	DNS Suffix(es)
protected-vm-10301		vcenter-server-site-A	1									::ffff:192.168.0.251	
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1				1.1.1.1	

The information in this CSV file applies different IP settings to vm-3-win on the protected site and on the recovery site.

- On site vcenter-server-site-B:
  - Sets the DNS suffixes example.com and eng.example.com for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, that sets a static IPv4 address 192.168.1.21, uses DHCP to obtain an IPv6 address, and uses DNS server 1.1.1.1.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, that uses DHCP to obtain an IPv4 address, sets a static IPv6 address ::ffff:192.168.1.22, and uses DNS server 1.1.1.2.
- On site vcenter-server-site-A:
  - Sets the DNS suffixes to example.com and eng.example.com for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, that uses DHCP to obtain an IPv4 address and sets a static IPv6 address ::ffff:192.168.1.22. Adapter ID 1 uses static IPv6 DNS servers ::ffff:192.168.0.250 and ::ffff:192.168.0.251.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 1.2.3.4 and 1.2.3.5, a static IPv4 address 192.168.0.22, and DNS server 1.1.1.1. By leaving the IPv6 column blank, Adapter ID 2 uses DHCP for IPv6 addresses.

Run DR IP Customizer to Customize IP Properties for Multiple Virtual Machines

You can use the DR IP Customizer tool to customize the IP properties for multiple virtual machines that Site Recovery Manager protects.

NOTE This release of Site Recovery Manager allows you to define subnet-level IP mapping rules to customize IP settings on virtual machines, as well as by using the DR IP Customizer tool. You can use subnet-level IP mapping rules in combination with DR IP Customizer. For information about how you can use subnet-level IP mapping rules and DR IP Customizer together, see "Customizing IP Properties for Multiple Virtual Machines," on page 67.

Prerequisites

Use the DR IP Customizer tool on a computer with access to vCenter Server instances in your environment.

Procedure

1 Open a command shell on the Site Recovery Manager Server host.

2 Change directory to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`.

3 Run the `dr-ip-customizer.exe` command to generate a comma-separated value (CSV) file that contains information about the protected virtual machines.

```
dr-ip-customizer.exe
--cfg ..\config\vmware-dr.xml
--cmd generate
--out "path_to_CSV_file.csv"
--vc vcenter_server_address
```

This example points `dr-ip-customizer.exe` to the `vmware-dr.xml` file of the Site Recovery Manager Server and generates the file *`path_to_CSV_file`*`.csv` for the vCenter Server instance at *vcenter_server_address*.

4 (Optional) Check the vCenter Server thumbprint and enter **`y`** to confirm that you trust this vCenter Server instance.

If you specified the `--ignore-thumbprint` option, you are not prompted to check the thumbprint.

5 Enter the login credentials for the vCenter Server instance.

You might be prompted again to confirm that you trust this vCenter Server instance.

6 Edit the generated CSV file to customize the IP properties for the virtual machines in the recovery plan.

You can use a spread sheet application to edit the CSV file. Save the modified CSV file under a new name.

7 Run `dr-ip-customizer.exe` to apply the customized IP properties from the modified CSV file.

You can run the DR IP Customizer tool on either the protected site or on the recovery site. Virtual machine IDs for protected virtual machines are different at each site, so whichever site you use when you run the DR IP Customizer tool to generate the CSV file, you must use the same site when you run DR IP Customizer again to apply the settings.

```
dr-ip-customizer.exe
--cfg ..\config\vmware-dr.xml
--cmd apply
--csv "path_to_CSV_file.csv"
--vc vcenter_server_address
```

This example points `dr-ip-customizer.exe` to the `vmware-dr.xml` file of the Site Recovery Manager Server and applies the customizations in the file *`path_to_CSV_file`*`.csv` to the vCenter Server instance at *vcenter_server_address*.

The specified customizations are applied to all of the virtual machines named in the CSV file during a recovery. You do not need to manually configure IP settings for these machines when you edit their recovery plan properties.

Customize IP Properties for Multiple Virtual Machines by Defining IP Customization Rules

You can specify a single subnet-level IP mapping rule for a selected configured virtual network mapping on the protected and recovery sites.

Subnet-level mapping eliminates the need to define exact adapter-level IP mapping. Instead, you specify an IP customization rule that Site Recovery Manager applies to relevant adapters. The IP customization rule is used for test and recovery workflows. You cannot reuse IP customization rules between different network mappings.

IMPORTANT IP subnet mapping rules support IPv4 only. Rule-based IPv6 customization is not supported inSite Recovery Manager. Site Recovery Manager does not evaluate IP mapping rules for virtual machines configured to use manual IP customization.

The IP customization rule applies to virtual machines failing over from a protected site IPv4 subnet to a recovery site IPv4 subnet, for example, from 10.17.23.0/24 to 10.18.22.0/24. The IP customization rule states that during recovery Site Recovery Manager evaluates the existing IP configuration of the recovered virtual machine's NICs and reconfigures static NICs found on the 10.17.23.0/24 subnet for the 10.18.22.0/24 subnet.

If the rule matches, Site Recovery Manager derives the new static IPv4 address from the old one by preserving the host bits of the original IPv4 address and placing it to the target subnet. For example, if the original protected site address is 10.17.23.55/24, the new address is 10.18.22.55/24.

If the default gateway text box is empty, Site Recovery Manager derives the new gateway parameter from the original one by preserving the host bits of the original IPv4 address and placing it in the target subnet. For example, if the original protected site gateway is 10.17.23.1, the new gateway is 10.18.22.1. If you specify an explicit gateway parameter, Site Recovery Manager checks that the IPv4 address syntax is correct and applies it exactly.

Site Recovery Manager applies DNS and other parameters as specified. DHCP-enabled NICs are not subject to customization as their network configuration remains unchanged during recovery.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, select **Network Mappings**.

3 Select a network mapping for which to define a customization rule.

4 To define a rule, click **Add IP Customization Rule**.

5 Enter a name for the rule.

6 Specify the subnet IP ranges that map to the protected and recovery sites.

7 Specify the network settings for the recovery site network.

8 Click **OK** to save your changes.

Apply IP Customization Rules to a Virtual Machine

You can apply an IP customization rule to the recovery settings of a protected virtual machine.

When you apply an IP customization rule, you specify a single subnet IP mapping rule for each network mapping.

If you set the advanced setting option `recovery.useIpMapperAutomatically` to True and configure the IP mapping rule for virtual networks, then Site Recovery Manager evaluates the subnet IP mapping rules during recovery to customize the virtual machines. If you set this option to False, Site Recovery Manager does not evaluate the IP mapping rules during recovery. You can override the effect of this option for each virtual machine by using the **IP Customization** option.

The `recovery.useIpMapperAutomatically` default option is True. If you set it to Auto, Site Recovery Manager customizes the virtual machine by using the IP Customization rule.

Prerequisites

For the list of guest operating systems for which Site Recovery Manager supports IP customization, see the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**.

2 On the **Related Objects** tab, click **Virtual Machines**.

3 Right-click a virtual machine and click **Configure Recovery**.

4 Click **IP Customization**.

5 From the IP customization mode list, select **Use IP customization rules if applicable** and click **OK**.

Reprotecting Virtual Machines After a Recovery

7

After a recovery, the recovery site becomes the new protected site, but it is not protected yet. If the original protected site is operational, you can reverse the direction of protection to use the original protected site as a new recovery site to protect the new protected site.

Manually reestablishing protection in the opposite direction by recreating all protection groups and recovery plans is time consuming and prone to errors. Site Recovery Manager provides the reprotect function, which is an automated way to reverse protection.

After Site Recovery Manager performs a recovery, the protected virtual machines start up on the recovery site. Because the former protected site might be offline, these virtual machines are not protected. By running reprotect when the protected site comes back online, you reverse the direction of replication to protect the recovered virtual machines on the recovery site back to the original protected site.

Reprotect uses the protection information that you established before a recovery to reverse the direction of protection. You can initiate the reprotect process only after recovery finishes without any errors. If the recovery finishes with errors, you must fix all errors and rerun the recovery, repeating this process until no errors occur.

You can conduct tests after a reprotect operation completes, to confirm that the new configuration of the protected and recovery sites is valid.

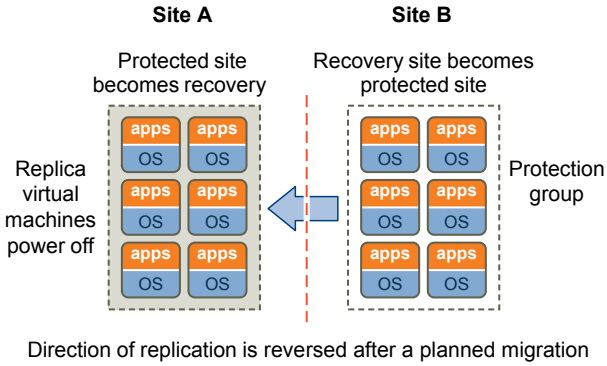
You can perform reprotect on protection groups that contain virtual machines that are configured for both array-based replication and for vSphere Replication.

Example: Performing a Reprotect Operation

Site A is the protected site and site B is the recovery site. If site A goes offline, run the disaster recovery workflow on the recovery plan to bring the virtual machines online on site B. After the recovery, the protected virtual machines from site A start up on site B without protection.

When site A comes back online, complete recovery by doing a planned migration because site A virtual machines and datastores need to be powered down and unmounted before reversing protection. Then initiate a reprotect operation to protect the recovered virtual machines on site B. Site B becomes the protected site, and site A becomes the recovery site. Site Recovery Manager reverses the direction of replication from site B to site A.

Figure 7-1. Site Recovery Manager Reprotect Process



- How Site Recovery Manager Reprotects Virtual Machines with Array Based Replication on page 84

  In the reprotect process with array based replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

- How Site Recovery Manager Reprotects Virtual Machines with vSphere Replication on page 85

  In the reprotect process using vSphere Replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

- Preconditions for Performing Reprotect on page 85

  You can perform reprotect only if you meet certain preconditions.

- Reprotect Virtual Machines on page 85

  Reprotect results in the reconfiguration of Site Recovery Manager protection groups and recovery plans to work in the opposite direction. After a reprotect operation, you can recover virtual machines back to the original site using a planned migration workflow.

- Reprotect States on page 86

  The reprotect process passes through several states that you can observe in the recovery plan in the Site Recovery Manager plug-in in the vSphere Client.

How Site Recovery Manager Reprotects Virtual Machines with Array Based Replication

In the reprotect process with array based replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

When you initiate the reprotect process, Site Recovery Manager instructs the underlying storage arrays to reverse the direction of replication. After reversing the replication, Site Recovery Manager creates placeholder virtual machines at the new recovery site, which was the original protected site before the reprotect.

When creating placeholder virtual machines on the new protected site, Site Recovery Manager uses the location of the original protected virtual machine to determine where to create the placeholder virtual machine. Site Recovery Manager uses the identity of the original protected virtual machine to create the placeholder. If the original protected virtual machines are no longer available, Site Recovery Manager uses the inventory mappings from the original recovery site to the original protected site to determine the resource pools and folders for the placeholder virtual machines. You must configure inventory mappings on both sites before running the reprotect process, or the process might fail.

When reprotecting virtual machines with array-based replication, Site Recovery Manager places the files for the placeholder virtual machines in the placeholder datastore for the original protected site, not in the datastore that held the original protected virtual machines.

Forcing synchronization of data from the new protection site to the new recovery site ensures that the recovery site has a current copy of the protected virtual machines running at the protection site. Forcing this synchronization ensures that recovery is possible immediately after the reprotect process finishes.

To learn how Site Recovery Manager reprotects virtual machines with vSphere Replication, see "How Site Recovery Manager Reprotects Virtual Machines with vSphere Replication," on page 85.

How Site Recovery Manager Reprotects Virtual Machines with vSphere Replication

In the reprotect process using vSphere Replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

When performing reprotection with vSphere Replication, Site Recovery Manager uses the original VMDK files as initial copies during synchronization. The full synchronization that appears in the recovery steps mostly performs checksums, and only a small amount of data is transferred through the network.

Forcing synchronization of data from the new protection site to the new recovery site ensures that the recovery site has a current copy of the protected virtual machines running at the protection site. Forcing this synchronization ensures that recovery is possible immediately after the reprotect process finishes.

Preconditions for Performing Reprotect

You can perform reprotect only if you meet certain preconditions.

You can perform reprotect on protection groups that contain virtual machines that are configured for both array-based replication and for vSphere Replication.

Before you can run reprotect, you must satisfy the preconditions.

1. Run a planned migration and make sure that all steps of the recovery plan finish successfully. If errors occur during the recovery, resolve the problems that caused the errors and rerun the recovery. When you rerun a recovery, operations that succeeded previously are skipped. For example, successfully recovered virtual machines are not recovered again and continue running without interruption.
2. The original protected site must be available. The vCenter Server instances, ESXi Servers, Site Recovery Manager Server instances, and corresponding databases must all be recoverable.
3. If you performed a disaster recovery operation, you must perform a planned migration when both sites are running again. If errors occur during the attempted planned migration, you must resolve the errors and rerun the planned migration until it succeeds.

Reprotect is not available under certain circumstances.

- Recovery plans cannot finish without errors. For reprotect to be available, all steps of the recovery plan must finish successfully.
- You cannot restore the original site, for example if a physical catastrophe destroys the original site. To unpair and recreate the pairing of protected and recovery sites, both sites must be available. If you cannot restore the original protected site, you must reinstall Site Recovery Manager on the protected and recovery sites.

Reprotect Virtual Machines

Reprotect results in the reconfiguration of Site Recovery Manager protection groups and recovery plans to work in the opposite direction. After a reprotect operation, you can recover virtual machines back to the original site using a planned migration workflow.

Prerequisites

See "Preconditions for Performing Reprotect," on page 85.

Procedure

1 In the vSphere Web Client, select **Site Recovery > Recovery Plans**.

2 Right-click a recovery plan and select **Reprotect**.

3 Select the check box to confirm that you understand that the reprotect operation is irreversible.

4 (Optional) Select the **Force Cleanup** check box to ignore errors during the cleanup operation on the recovery site, and click **Next**.

The **Force Cleanup** option is only available after you have performed an initial reprotect operation that has experienced errors.

5 Review the reprotect information and click **Finish**.

6 Click **Monitor > Recovery Steps** tab to monitor the progress of the reprotect operation.

Site Recovery Manager reverses the recovery site and protected sites. Site Recovery Manager creates placeholder copies of virtual machines from the new protected site at the new recovery site.

Reprotect States

The reprotect process passes through several states that you can observe in the recovery plan in the Site Recovery Manager plug-in in the vSphere Client.

If reprotect fails, or succeeds partially, you can perform remedial actions to complete the reprotect.

Table 7-1. Reprotect States

State	Description	Remedial Action
Reprotect In Progress	Site Recovery Manager is running reprotect.	None
Partial Reprotect	Occurs if multiple recovery plans share the same protection groups and reprotect succeeds for some groups in some plans, but not for others.	Run reprotect again on the partially reprotected plans.
Incomplete Reprotect	Occurs because of failures during reprotect. For example, this state might occur because of a failure to synchronize storage or a failure to create placeholder virtual machines.	■ If a reprotect operation fails to synchronize storage, make sure that sites are connected, review the reprotect progress in the vSphere Client , and start the reprotect task again. If reprotect still won't complete, run the reprotect task with the **Force Cleanup** option. ■ If Site Recovery Manager fails to create placeholder virtual machines, recovery is still possible. Review the reprotect steps in the vSphere Client, resolve any open issues, and start the reprotect task again.
Reprotect Interrupted	Occurs if one of the Site Recovery Manager Servers stops unexpectedly during the reprotect process.	Ensure that both Site Recovery Manager Servers are running and start the reprotect task again.

Restoring the Pre-Recovery Site Configuration By Performing Failback

8

To restore the original configuration of the protected and recovery sites after a recovery, you can perform a sequence of optional procedures known as failback.

After a planned migration or a disaster recovery, the former recovery site becomes the protected site. Immediately after the recovery, the new protected site has no recovery site to which to recover. If you run reprotect, the new protected site is protected by the original protection site, reversing the original direction of protection. See Chapter 7, "Reprotecting Virtual Machines After a Recovery," on page 83 for information about reprotect.

To restore the configuration of the protected and recovery sites to their inital configuration before the recovery, you perform failback.

To perform failback, you run a sequence of reprotect and planned migration operations.

1 Perform a reprotect. The recovery site becomes the protected site. The former protected site becomes the recovery site.

2 Perform a planned migration to shut down the virtual machines on the protected site and start up the virtual machines on the recovery site. To avoid interruptions in virtual machine availability, you might want to run a test before you start the planned migration. If the test identifies errors, you can resolve them before you perform the planned migration.

3 Perform a second reprotect, to revert the protected and recovery sites to their original configuration before the recovery.

You can configure and run a failback when you are ready to restore services to the original protected site, after you have brought it back online after an incident.

Example: Performing a Failback Operation

Site A is the protected site and B is the recovery site. A recovery occurs, migrating the virtual machines from site A to site B. To restore site A as the protected site, you perform a failback.

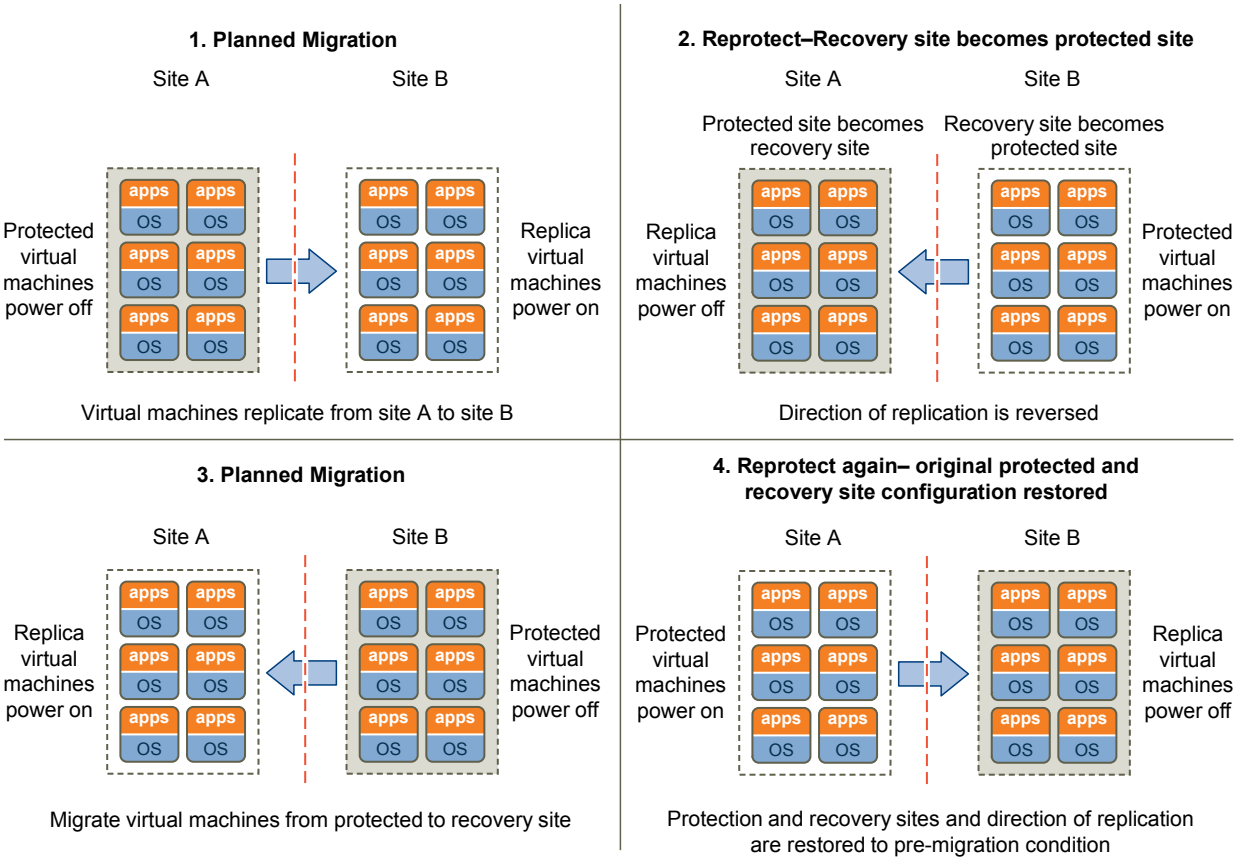
1 Virtual machines replicate from site A to site B.

2 Perform a reprotect. Site B, the former recovery site, becomes the protected site. Site Recovery Manager uses the protection information to establish the protection of site B. Site A becomes the recovery site.

3 Perform a planned migration to recover the protected virtual machines on site B to site A.

4 Perform a second reprotect. Site A becomes the protected site and site B becomes the recovery site.

Figure 8-1. Site Recovery Manager Failback Process



Perform a Failback

After Site Recovery Manager performs a recovery, you can perform a failback to restore the original configuration of the protected and recovery sites.

To aid comprehension, the original protected site from before a recovery is site A. The original recovery site is site B. After a recovery from site A to site B, the recovered virtual machines are running on site B without protection.

Prerequisites

Verify that the following conditions are in place.

- You have performed a recovery, either as part of a planned migration or as part of a disaster recovery.
- The original protected site, site A, is running.
- If you performed a disaster recovery, you must perform a planned migration recovery when the hosts and datastores on the original protected site, site A, are running again.
- You did not run reprotect since the recovery.

Procedure

1. In the vSphere Web Client, select **Site Recovery > Recovery Plans**.
2. Right-click a recovery plan and select **Reprotect**.
3. Select the check box to confirm that you understand that the reprotect operation is irreversible and click **Next**.

4 Determine whether to enable **Force Cleanup** and click **Next**.

   This option is only available after you have run reprotect once and errors occured. Enabling this option forces the removal of virtual machines, ignoring errors, and returns the recovery plan to the ready state.

5 Review the reprotect information and click **Finish**.

6 In the **Monitor** tab, click **Recovery Steps** to monitor the reprotect operation until it finishes.

7 (Optional) If necessary, rerun reprotect until it finishes without errors.

   At the end of the reprotect operation, Site Recovery Manager has reversed replication, so that the original recovery site, site B, is now the protected site.

8 (Optional) After the test completes, right-click the recovery plan and select **Cleanup** to clean up the recovery plan.

9 Right-click the recovery plan and select **Recovery** to run the recovery plan as a planned migration.

10 In the **Monitor** tab, click **Recovery Steps** to monitor the planned migration until it finishes.

   The planned migration shuts down the virtual machines on the new protected site, site B, and starts up the virtual machines on the new recovery site, site A. If necessary, rerun the planned migration until it finishes without errors.

   When the planned migration completes, the virtual machines are running on the original protected site, site A, but the virtual machines are not protected. The virtual machines on the original recovery site, site B, are powered off.

11 Right-click the recovery plan and select **Reprotect** and follow the instructions of the wizard to perform a second reprotect operation.

   Running reprotect again reestablishes protection in the original direction from before the recovery.

You restored the protected and recovery sites to their original configuration before the recovery. The protected site is site A, and the recovery site is site B.

Interoperability of Site Recovery Manager with Other Software

9

Site Recovery Manager Server operates as an extension to the vCenter Server at a site.
Site Recovery Manager is compatible with other VMware solutions, and with third-party software.

You can run other VMware solutions such as vCenter Update Manager, vCenter Server Heartbeat, VMware Fault Tolerance, vSphere Storage vMotion, vSphere Storage DRS, and vCenter CapacityIQ in deployments that you protect using Site Recovery Manager. Use caution before you connect other VMware solutions to the vCenter Server instance to which the Site Recovery Manager Server is connected. Connecting other VMware solutions to the same vCenter Server instance as Site Recovery Manager might cause problems when you upgrade Site Recovery Manager or vSphere. Check the compatibility and interoperability of the versions of these solutions with your version of Site Recovery Manager by consulting *VMware Product Interoperability Matrixes*.

This chapter includes the following topics:

Site Recovery Manager and vCenter Server

Site Recovery Manager takes advantage of vCenter Server services, such as storage management, authentication, authorization, and guest customization. Site Recovery Manager also uses the standard set of vSphere administrative tools to manage these services.

Because the Site Recovery Manager Server depends on vCenter Server for some services, you must install and configure vCenter Server at a site before you install Site Recovery Manager.

You can use Site Recovery Manager and vSphere Replication with the vCenter Server Appliance or with a standard vCenter Server installation. You can have vCenter Server Appliance on one site and a standard vCenter Server installation on the other.

How Changes to vCenter Server Inventory Affect Site Recovery Manager

Because Site Recovery Manager protection groups apply to a subset of the vCenter Server inventory, changes to the protected inventory made by vCenter Server administrators and users can affect the integrity of Site Recovery Manager protection and recovery. Site Recovery Manager depends on the availability of certain objects, such as virtual machines, folders, resource pools, and networks, in the vCenter Server inventory at the protected and recovery sites. Deletion of resources such as folders or networks that are referenced by recovery plans can invalidate the plan. Renaming or relocating objects in the vCenter Server inventory does not affect Site Recovery Manager, unless it causes resources to become inaccessible during test or recovery.

Site Recovery Manager can tolerate certain changes at the protected site without disruption.

- Deleting protected virtual machines.
- Deleting an object for which an inventory mapping exists.

Site Recovery Manager can tolerate certain changes at the recovery site without disruption.

- Moving placeholder virtual machines to a different folder or resource pool.
- Deleting an object for which an inventory map exists.

Site Recovery Manager and the vCenter Server Database

If you update the vCenter Server installation that Site Recovery Manager extends, do not reinitialize the vCenter Server database during the update. Site Recovery Manager stores identification information about all vCenter Server objects in the Site Recovery Manager database. If you reinitialize the vCenter Server database, the identification data that Site Recovery Manager has stored no longer matches identification information in the new vCenter Server instance and objects are not found.

How Site Recovery Manager Interacts with DPM and DRS During Recovery

Distributed Power Management (DPM) and Distributed Resource Scheduler (DRS) are not mandatory, but Site Recovery Manager supports both services and enabling them provides certain benefits when you use Site Recovery Manager.

DPM is a VMware feature that manages power consumption by ESX hosts. DRS is a VMware facility that manages the assignment of virtual machines to ESX hosts.

Site Recovery Manager temporarily disables DPM for the clusters on the recovery site and ensures that all hosts in the cluster are powered on when recovery or test recovery starts. This allows for sufficient host capacity while recovering virtual machines. After the recovery or test is finished, Site Recovery Manager restores the DPM settings on the cluster on the recovery site to their original values.

For planned migration and reprotect operations, Site Recovery Manager also disables DPM on the affected clusters on the protected site and ensures that all of the hosts in the cluster are powered on. This allows Site Recovery Manager to complete host level operations, for example unmounting datastores or cleaning up storage after a reprotect operation. After the planned migration or reprotect operation has finished, Site Recovery Manager restores the DPM settings on the cluster on the protected site to their original values.

The hosts in the cluster are left in the running state so that DPM can power them down as needed. Site Recovery Manager registers virtual machines across the available ESX hosts in a round-robin order, to distribute the potential load as evenly as possible. Site Recovery Manager always uses DRS placement to balance the load intelligently across hosts before it powers on recovered virtual machines on the recovery site, even if DRS is disabled on the cluster.

If DRS is enabled and in fully automatic mode, DRS might move other virtual machines to further balance the load across the cluster while Site Recovery Manager is powering on the recovered virtual machines. DRS continues to balance all virtual machines across the cluster after Site Recovery Manager has powered on the recovered virtual machines.

How Site Recovery Manager Interacts with Storage DRS or Storage vMotion

You can use Site Recovery Manager when protecting virtual machines on sites that are configured for Storage DRS or Storage vMotion if you follow certain guidelines.

The behavior of Storage DRS or Storage vMotion depends on whether you use Site Recovery Manager with array-based replication or with vSphere Replication.

Using Site Recovery Manager with Array-Based Replication on Sites with Storage DRS or Storage vMotion

You must follow the guidelines if you use array-based replication to protect virtual machines on sites that use Storage DRS or Storage vMotion.

- If your storage array supports consistency groups, Site Recovery Manager is compatible with vSphere Storage DRS and vSphere Storage vMotion. You can use Storage DRS and Storage vMotion to move virtual machine files within a consistency group that Site Recovery Manager protects. If your storage array does not support consistency groups, you cannot use Storage DRS and Storage vMotion in combination with Site Recovery Manager.
- If you enable Storage DRS on the protection site, a datastore cluster must contain one and only one consistency group. Do not include any datastore that does not belong to the consistency group in the cluster. Placing multiple consistency groups into the same cluster might result in virtual machines being lost during a recovery. This guideline also applies on the recovery site if Storage DRS is enabled on the recovery site.
- Do not use Storage DRS or Storage vMotion to move virtual machines regularly. Do not accept recommendations to manually move virtual machines regularly. You can move virtual machines occasionally, but excessive movement of virtual machines can cause problems. Moving virtual machines requires the array to replicate virtual machines over the network, which takes time and consumes bandwidth. When Storage DRS or Storage vMotion moves virtual machines, you might encounter problems during a recovery:
  - If Storage DRS or Storage vMotion moves a virtual machine to a different consistency group within the same protection group, there is a short period between Site Recovery Manager propagating the new location of the virtual machine to the recovery site and the array replicating the changes to the recovery site. In addition, there is another period during which the arrays replicate the source and target consistency groups to a consistent state on the recovery site. While the array is propagating all of the changes to the recovery site, disaster recovery of this virtual machine might fail.
  - If Storage DRS or Storage vMotion moves a virtual machine to a different protection group, Site Recovery Manager generates a protection error for this virtual machine. You must unconfigure protection of the virtual machine in the old protection group and configure protection of the virtual machine in the new protection group. Until you configure protection in the new protection group, planned migration or disaster recovery of this virtual machine fails.
- Adding a disk to a protected virtual machine results in the same problems as for moving an entire virtual machine. Site Recovery Manager does not prevent you from doing this, but if a virtual machine contains an unreplicated disk and you do not exclude the disk from protection, powering on the virtual machine fails after the move.

- Moving a protected disk to a different consistency group results in the same problems as for moving an entire virtual machine. These problems occur if you move a disk to a different consistency group within the same protection group or if you move it into a different protection group. Site Recovery Manager does not prevent you from doing this, but if a disk has moved to a different consistency group, powering on the virtual machine fails after the move.

Using Site Recovery Manager with vSphere Replication on Sites with Storage DRS or Storage vMotion

You must follow the guidelines if you use vSphere Replication to protect virtual machines on sites that use Storage DRS or Storage vMotion.

- vSphere Replication is compatible with vSphere Storage vMotion and vSphere Storage DRS on the protected site. You can use Storage vMotion and Storage DRS to move the disk files of a virtual machine that vSphere Replication protects, with no impact on replication.
- vSphere Replication is compatible with Storage vMotion and saves the state of a disk or virtual machine when the home directory of a disk or virtual machine moves. Replication of the disk or virtual machine continues normally after the move.
- A full sync causes Storage DRS to trigger Storage vMotion only if you set the Storage DRS rules to be very aggressive, or if a large number of virtual machines perform a full sync at the same time. The default I/O latency threshold for Storage DRS is 15ms. By default, Storage DRS performs loading balancing operations every 8 hours. Storage DRS also waits until it has collected sufficient statistics about the I/O load before it generates Storage vMotion recommendations. Consequently, a full sync only affects Storage DRS recommendations if the full sync lasts for a long time and if, during that time, the additional I/O that the full sync generates causes the latency to exceed the I/O latency threshold.

How Site Recovery Manager Interacts with vSphere High Availability

You can use Site Recovery Manager to protect virtual machines on which vSphere High Availability (HA) is enabled.

HA protects virtual machines from ESXi host failures by restarting virtual machines from hosts that fail on new hosts within the same site. Site Recovery Manager protects virtual machines against full site failures by restarting the virtual machines at the recovery site. The key difference between HA and Site Recovery Manager is that HA operates on individual virtual machines and restarts the virtual machines automatically. Site Recovery Manager operates at the recovery plan level and requires a user to initiate a recovery manually.

To transfer the HA settings for a virtual machine onto the recovery site, you must set the HA settings on the placeholder virtual machine before performing recovery, at any time after you have configured the protection of the virtual machine.

You can replicate HA virtual machines by using array-based replication or vSphere Replication. If HA restarts a protected virtual on another host on the protected site, vSphere Replication will perform a full sync after the virtual machine restarts.

Site Recovery Manager does not require HA as a prerequisite for protecting virtual machines. Similarly, HA does not require Site Recovery Manager.

Site Recovery Manager and vSphere PowerCLI

VMware vSphere PowerCLI provides a Windows PowerShell interface for command-line access to Site Recovery Manager tasks.

vSphere PowerCLI exposes the Site Recovery Manager APIs. You can use vSphere PowerCLI to administrate Site Recovery Manager or to create scripts that automate Site Recovery Manager tasks.

For information about how to manage Site Recovery Manager by using vSphere PowerCLI, see the vSphere PowerCLI documentation at https://www.vmware.com/support/developer/PowerCLI/.

Site Recovery Manager and vCenter Orchestrator

The vCenter Orchestrator plug-in for vCenter Site Recovery Manager allows you to automate certain Site Recovery Manager operations by including them in vCenter Orchestrator workflows.

The vCenter Orchestrator plug-in for vCenter Site Recovery Manager includes actions and workflows that run Site Recovery Manager operations. If you are a vCenter Orchestrator administrator, you can create workflows that include the actions and workflows from the Site Recovery Manager plug-in. By including Site Recovery Manager actions and workflows in vCenter Orchestrator workflows, you can combine Site Recovery Manager operations with the automated operations that other vCenter Orchestrator plug-ins provide.

For example, you can create a workflow that uses the actions and workflows of the vCenter Orchestrator plug-in for vCenter Server to create and configure virtual machines and register them with vCenter Server. In the same workflow, you can use the actions and workflows from the Site Recovery Manager plug-in to create protection groups and protect the virtual machines as soon as they are created. You can also use Site Recovery Manager actions and workflows to configure some of the recovery settings for the protected virtual machines. Combining the vCenter Server and Site Recovery Manager actions and workflows in a vCenter Orchestrator workflow thus allows you to automate the process of creating and protecting virtual machines.

You can use the vCenter Orchestrator plug-in for vCenter Site Recovery Manager in a shared recovery site configuration, in which you connect multiple Site Recovery Manager instances to a single vCenter Server instance. You can also use the vCenter Orchestrator plug-in for vCenter Site Recovery Manager with multiple Site Recovery Manager instances on multiple vCenter Server instances that are connected to the same vCenter Single Sign-On server.

For information about creating workflows by using vCenter Orchestrator, see the vCenter Orchestrator documentation.

For information about how to use the vCenter Orchestrator plug-in for vCenter Site Recovery Manager, see the vCenter Orchestrator Plug-Ins Documentation.

Automated Operations That the vCenter Orchestrator Plug-In for Site Recovery Manager Provides

With the vCenter Orchestrator plug-in for vCenter Site Recovery Manager, you can automate the creation of your Site Recovery Manager infrastructure, to add virtual machines to protection groups, and to configure the recovery settings of virtual machines.

With the vCenter Orchestrator plug-in for vCenter Site Recovery Manager you can protect virtual machines by adding them to array-based replication or to vSphere Replication protection groups. The plug-in does not automate the configuration of vSphere Replication on virtual machines. You must manually configure vSphere Replication on virtual machines.

Because of the significant effect that running a recovery has on the protected and recovery sites, you cannot use the vCenter Orchestrator plug-in for vCenter Site Recovery Manager to automate test recovery, planned migration, or disaster recovery. Recovery is too sensitive to automate and always requires human intervention.

The vCenter Orchestrator plug-in for vCenter Site Recovery Manager includes vCenter Orchestrator actions, workflows, policy templates to trigger actions when certain events occur, and scripting objects to expose selected elements of the Site Recovery Manager API to workflows.

- The plug-in provides actions and workflows that create a Site Recovery Manager infrastructure:
  - Create array-based protection groups and vSphere Replication protection groups
  - Create inventory mappings between matching objects
  - Add protection groups to existing recovery plans
- The plug-in provides actions and workflows that protect virtual machines:
  - Protect a virtual machine by using an existing array-based protection group
  - Protect a virtual machine by using an existing vSphere Replication protection group
- The plug-in provides actions and workflows that configure recovery settings on virtual machines:
  - Set the recovery priority
  - Create per-virtual machine recovery steps
  - Set the final power state of a recovered virtual machine
- The plug-in provides actions and workflows that obtain information from Site Recovery Manager Server:
  - List protected datastores
  - List protection groups and recovery plans
  - Find array-based protection groups by datastore
  - Get unassigned replication datastores and recovery plan states

Protecting Microsoft Cluster Server and Fault Tolerant Virtual Machines

You can use Site Recovery Manager to protect Microsoft Cluster Server (MSCS) and fault tolerant virtual machines, with certain limitations.

To use Site Recovery Manager to protect MSCS and fault tolerant virtual machines, you might need to change your environment.

General Limitations to Protecting MSCS and Fault Tolerant Virtual Machines

Protecting MSCS and fault tolerant virtual machines is subject to the following limitations.

- You can use array-based replication only to protect MSCS virtual machines. Protecting MSCS virtual machines with vSphere Replication is not supported.
- Reprotect of MSCS or fault tolerant virtual machines requires VMware High Availability (HA) and VMware Distributed Resource Scheduler (DRS). When you move MSCS or fault tolerant virtual machines across their primary and secondary sites during reprotect, you must enable HA and DRS, and set the affinity and antiaffinity rules as appropriate. See "DRS Requirements for Protection of MSCS Virtual Machines," on page 97.
- vSphere does not support vSphere vMotion for MSCS virtual machines.

ESXi Host Requirements for Protection of MSCS Virtual Machines

To protect MSCS or fault tolerant virtual machines, the ESXi host machines on which the virtual machines run must meet certain criteria.

- You must run a fault tolerant virtual machine and its shadow on two separate ESXi Server instances.
- You can run a cluster of MSCS virtual machines in the following possible configurations.

Cluster-in-a-box The MSCS virtual machines in the cluster run on a single ESXi Server. You can have a maximum of five MSCS nodes on one ESXi Server.

Cluster-across-boxes You can spread the MSCS cluster across a maximum of five ESXi Server instances. You can protect only one virtual machine node of any MSCS cluster on a single ESXi Server instance. You can have multiple MSCS node virtual machines running on an ESXi host, as long as they do not participate in the same MSCS cluster. This configuration requires shared storage on a Fibre Channel SAN for the quorum disk.

DRS Requirements for Protection of MSCS Virtual Machines

To use DRS on sites that contain MSCS virtual machines, you must configure the DRS rules to allow Site Recovery Manager to protect the virtual machines. By following the guidelines, you can protect MSCS virtual machines on sites that run DRS if the placeholder virtual machines are in either a cluster-across-boxes MSCS deployment or in a cluster-in-a-box MSCS deployment.

- Because vSphere does not support vSphere vMotion for MSCS virtual machines, you must set the `VM to Host` DRS rule so that DRS does not perform vMotion on MSCS nodes. Set the `VM to Host` rule for the virtual machines on the protected site and for the shadow virtual machines on the recovery site.
- Set the DRS rules on the virtual machines on the protected site before you configure MSCS in the guest operating systems. Set the DRS rules immediately after you deploy, configure, or power on the virtual machines.
- Set the DRS rules on the virtual machines on the recovery site immediately after you create a protection group of MSCS nodes, as soon as the placeholder virtual machines appear on the recovery site.
- DRS rules that you set on the protected site are not transferred to the recovery site after a recovery. For this reason, you must set the DRS rules on the placeholder virtual machines on the recovery site.
- Do not run a test recovery or a real recovery before you set the DRS rules on the recovery site.

If you do not follow the guidelines on either the protected site or on the recovery site, vSphere vMotion might move MSCS virtual machines to a configuration that Site Recovery Manager does not support.

- In a cluster-in-a-box deployment on either the protected or recovery site, vSphere vMotion might move MSCS virtual machines to different ESXi hosts.
- In a cluster-in-a-box deployment on either the protected or recovery site, vSphere vMotion might move some or all of the MSCS virtual machines to a single ESXi host.

Limitations to Protection and Recovery of Virtual Machines

The protection and recovery by Site Recovery Manager of virtual machines is subject to limitations.

Protection and Recovery of Suspended Virtual Machines

When you suspend a virtual machine, vSphere creates and saves its memory state. When the virtual machine resumes, vSphere restores the saved memory state to allow the virtual machine to continue without any disruption to the applications and guest operating systems that it is running.

Protection and Recovery of Virtual Machines with Snapshots

Array-based replication supports the protection and recovery of virtual machines with snapshots, but with limitations.

You can specify a custom location for storing snapshot delta files by setting the `workingDir` parameter in VMX files. Site Recovery Manager does not support the use of the `workingDir` parameter.

Limitations also apply if you are running versions of ESX or ESXi Server older than version 4.1.

- If the virtual machine has multiple VMDK disk files, all the disk files must be contained in the same folder as the VMX file itself.
- If a virtual machine is attached to a Raw Disk Mapping (RDM) disk device, you must store the mapping file in the same folder as the VMX file. RDM snapshots are only available if you create the RDM mapping using Virtual Compatibility Mode.

If you are running a ESX or ESXi Server 4.1 or later, these limitations do not apply.

vSphere Replication supports the protection of virtual machines with snapshots, but you can only recover the latest snapshot. vSphere Replication erases the snapshot information in the recovered virtual machine. As a consequence, snapshots are no longer available after recovery, unless you configure vSphere Replication to retain multiple point-in-time snapshots. For information about recovering older snapshots by using multiple point-in-time snapshots with vSphere Replication, see "Replicating a Virtual Machine and Enabling Multiple Point in Time Instances," on page 27.

Protection and Recovery of Virtual Machines with Memory State Snapshots

When protecting virtual machines with memory state snapshots, the ESXi hosts at the protection and recovery sites must have compatible CPUs, as defined in the VMware knowledge base articles VMotion CPU Compatibility Requirements for Intel Processors and VMotion CPU Compatibility Requirements for AMD Processors. The hosts must also have the same BIOS features enabled. If the BIOS configurations of the servers do not match, they show a compatibility error message even if they are otherwise identical. The two most common features to check are Non-Execute Memory Protection (NX / XD) and Virtualization Technology (VT / AMD-V).

Protection and Recovery of Linked Clone Virtual Machines

vSphere Replication does not support the protection and recovery of virtual machines that are linked clones.

Array-based replication supports the protection and recovery of virtual machines that are linked clones if all the nodes in the snapshot tree are replicated.

Protection and Recovery of Virtual Machines with Reservations, Affinity Rules, or Limits

When Site Recovery Manager recovers a virtual machine to the recovery site, it does not preserve any reservations, affinity rules, or limits that you have placed on the virtual machine. Site Recovery Manager does not preserve reservations, affinity rules, and limits on the recovery site because the recovery site might have different resource requirements to the protected site.

You can set reservations, affinity rules, and limits for recovered virtual machines by configuring reservations and limits on the resource pools on the recovery site and setting up the resource pool mapping accordingly. Alternatively, you can set reservations, affinity rules, or limits manually on the placeholder virtual machines on the recovery site.

Protection and Recovery of Virtual Machines Attached to RDM Disk Devices

The protection and recovery of virtual machines that are attached to a raw disk mapping (RDM) disk device is subject to different support depending on whether you use array-based replication or vSphere Replication.

- Array-based replication supports RDM devices in physical compatibility mode and in virtual compatibility mode. If you use Site Recovery Manager with array-based repliction, you can protect and recover virtual machines that use RDM in either physical compatibility mode or virtual compatibility mode.
- vSphere Replication supports RDM devices in virtual mode only, for both the source and target device. If you use vSphere Replication, you cannot protect and recover virtual machines that use RDM in physical compatibility mode.
- If you use both array-based repliction and vSphere Replication, you can only protect and recover virtual machines that use RDM in physical compatibility mode by using array-based replication. You can protect and recover virtual machines that use RDM in virtual compatibility mode by using either array-based repliction or vSphere Replication.

Planned Migration of Virtual Machines on Datastores that Use SIOC

In previous releases of Site Recovery Manager you had to disable storage I/O control (SIOC) on datastores that you included in a recovery plan before you ran a planned migration. This release of Site Recovery Manager fully supports SIOC, so you do not have to disable SIOC before you run a planned migration.

Disaster Recovery and Reprotect of Virtual Machines on Datastores that Use SIOC

In previous releases of Site Recovery Manager, if you ran a disaster recovery with SIOC enabled, the recovery would succeed with errors. After the recovery, you had to manually disable SIOC on the protected site and run a planned migration recovery again. You could not run reprotect until you successfully ran a planned migration. This release of Site Recovery Manager fully supports SIOC, so recovery succeeds without errors and you can run planned migration and reprotect after a disaster recovery without disabling SIOC.

Protection and Recovery of Virtual Machines with Components on Multiple Arrays

Array-based replication in Site Recovery Manager depends on the concept of an array pair. Site Recovery Manager defines groups of datastores that it recovers as units. As a consequence, limitations apply to how you can store the components of virutal machines that you protect using array-based replication.

- Site Recovery Manager does not support storing virtual machine components on multiple arrays on the protected site that replicate to a single array on the recovery site.
- Site Recovery Manager does not support storing virtual machine components on multiple arrays on the protected site that replicate to mulitple arrays on the recovery site, if the virtual machine components span both arrrays.

If you replicate virtual machine components from multiple arrays to a single array or to a span of arrays on the recovery site, the VMX configurations of the UUID of the datastores on the protected site do not match the configurations on the recovery site.

The location of the VMX file of a virtual machine determines which array pair a virtual machine belongs to. A virtual machine cannot belong to two array pairs, so if it has more than one disk and if one of those disks is in an array that is not part of the array pair to which the virtual machine belongs, Site Recovery Manager cannot protect the whole virtual machine. Site Recovery Manager handles the disk that is not on the same array pair as the virtual machine as an unreplicated device.

As a consequence, store all the virtual disks, swap files, RDM devices, and the working directory for the virtual machine on LUNs in the same array so that Site Recovery Manager can protect all the components of the virtual machine.

Protection and Recovery of Active Directory Domain Controllers

Do not use Site Recovery Manager to protect Active Directory domain controllers. Active Directory provides its own replication technology and restore mode. Use the Active Directory replication technology and restore mode technologies to handle disaster recovery situations.

Using Site Recovery Manager with Admission Control Clusters

You can use Admission Control on a cluster to reserve resources on the recovery site. However, using Admission Control can affect disaster recovery by preventing Site Recovery Manager from powering on virtual machines when running a recovery plan. Admission Control can prevent virtual machines from powering on if powering them on would violate the relevant Admission Control constraints.

You can add a command step to a recovery plan to run a PowerCLI script that disables Admission Control during the recovery. See "Creating Custom Recovery Steps," on page 56 for information about creating command steps.

1 Create a pre-power on command step in the recovery plan that runs a PowerCLI script to disable Admission Control.

```
Get-Cluster cluster_name | Set-Cluster -HAAdmissionControlEnabled:$false
```

2 Create a post-power on command step in the recovery plan to reenable Admission Control after the virtual machine powers on.

```
Get-Cluster cluster_name | Set-Cluster -HAAdmissionControlEnabled:$true
```

If you disable Admission Control during recovery, you must manually reenable Admission Control after you perform cleanup following a test recovery. Disabling Admission Control might affect the ability of High Availability to restart virtual machines on the recovery site. Do not disable Admission Control for prolonged periods.

Advanced Site Recovery Manager Configuration 10

The Site Recovery Manager default configuration enables some simple recovery scenarios. Advanced users can customize Site Recovery Manager to support a broader range of site recovery requirements.

This chapter includes the following topics:

Reconfigure Site Recovery Manager Settings

Using the **Advanced Settings**, you can view or change many custom settings for the Site Recovery Manager service. Advanced Settings provide a way for a user with adequate privileges to change default values that affect the operation of various Site Recovery Manager features.

IMPORTANT During an upgrade, Site Recovery Manager does not retain any advanced settings that you configured in the previous installation. This is by design. Due to changes in default values or improvements in performance, advanced settings that you set in a previous version of Site Recovery Manager might not be required by or compatible with the new version. Similarly, if you uninstall then reinstall the same version of Site Recovery Manager, reusing the database from the previous installation, advanced settings are not retained.

Change Site Recovery Manager History Report Collection Setting

Site Recovery Manager history reports are useful to diagnose Site Recovery Manager Server behavior before and after a failure. You can change the number of history reports to export.

When you run failover, test, cleanup, and reprotect operations with site A as the protected site and site B as recovery site, you can export history reports for these operations when you collect a support bundle for Site B, the recovery site. The most recent history is fetched directly from the Site Recovery Manager database.

After reprotect occurs, site A is the new recovery site and site B is the protected site. When you run failover, test, cleanup, and reprotect operations, you can export history reports when you collect a support bundle for site A, the recovery site.

Prerequisites

- Verify that you have Administrator credentials.
- Site Recovery Manager must be connected to a Site Recovery Manager database that you can access with valid database credentials.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, click **Advanced Settings**.

3 Select **Export History** and click **Edit**.

4 Change the value for **exportHistory.numReports** as needed.

You can enter a value from 0 to 50. The default value is 5.

5 To choose not to export reports, change the value to zero (0).

6 Click **OK** to save your changes.

Change Local Site Settings

Site Recovery Manager monitors consumption of resources on the Site Recovery Manager Server host, and it raises an alarm if a resource threshold is reached. You can change the thresholds and the way that Site Recovery Manager raises the alarms.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, click **Advanced Settings**.

3 Click **Local Site Status**.

4 Click **Edit** to change the settings.

Option	Action
Change the interval at which Site Recovery Manager checks the CPU usage, disk space, and free memory at the local site. The default value is 60 seconds.	Enter a new value in the **localSiteStatus.checkInterval** text box.
Change the name of the local site.	Enter a new value in the **localSiteStatus.displayName** text box.
Change the timeout during which Site Recovery Manager waits between raising alarms about CPU usage, disk space, and free memory at the local site. The default value is 600 seconds.	Enter a new value in the **localSiteStatus.eventFrequency** text box.
Change the percentage of CPU usage that causes Site Recovery Manager to raise a high CPU usage event. The default value is 70.	Enter a new value in the **localSiteStatus.maxCpuUsage** text box.
Change the percentage of free disk space that causes Site Recovery Manager to raise a low disk space event. The default value is 100.	Enter a new value in the **localSiteStatus.minDiskSpace** text box.
Change the amount of free memory that causes Site Recovery Manager to raise a low memory event. The default value is 32 MB.	Enter a new value in the **localSiteStatus.minMemory** text box.

5 Click **OK** to save your changes.

Change Logging Settings

You can change the levels of logging that Site Recovery Manager provides for the Site Recovery Manager Server components.

Site Recovery Manager Server operates log rotation. When you restart Site Recovery Manager Server, or when a log file becomes large, Site Recovery Manager Server creates a new log file and writes subsequent log messages to the new log file. When Site Recovery Manager Server creates new log files, it compresses the old log files to save space.

You might reduce the logging levels for some Site Recovery Manager Server components because log files become too large too quickly. You might increase logging levels for certain components to help diagnose problems. The list of available logging levels is the same for all Site Recovery Manager Server components.

none	Turns off logging.
quiet	Records minimal log entries.
panic	Records only panic log entries. Panic messages occur in cases of complete failure.
error	Records panic and error log entries. Error messages occur in cases of problems that might or might not result in a failure.
warning	Records panic, error, and warning log entries. Warning messages occur for behavior that is undesirable but that might be part of the expected course of operation.
info	Records panic, error, warning, and information log entries. Information messages provide information about normal operation.
verbose	Records panic, error, warning, information, and verbose log entries. Verbose messages provide more detailed information than information messages.
trivia	Records panic, error, warning, information, verbose, and trivia log entries. Trivia messages provide all available information. This level of logging is useful for debugging but it can produce so much data that it might affect performance. **NOTE** Set this logging level only when instructed by VMware Support to help resolve a problem.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, click **Advanced Settings**.

3 Click **Log Manager**.

4 Click **Edit** to modify the logging settings.

By default, all components record verbose level logs, unless stated otherwise in the description of the logging level.

Option	Description
Set logging level for all components that do not have an entry in logManager. The default is verbose.	Select a logging level from the **logManager.Default** drop-down menu.
Set logging level for the external API module. The default is verbose.	Select a logging level from the **logManager.ExternalAPI** drop-down menu.
Set logging level for vSphere Replication. The default is verbose.	Select a logging level from the **logManager.HbrProvider** drop-down menu.
Set logging level for the IP Customizer tool. The default is verbose.	Select a logging level from the **logManager.IPCustomizer** drop-down menu.
Set logging level for inventory mapping. The default is verbose.	Select a logging level from the **logManager.InventoryMapper** drop-down menu.
Set logging level for licensing issues. The default is verbose.	Select a logging level from the **logManager.Licensing** drop-down menu.
Set logging level for persistence issues. The default is verbose.	Select a logging level from the **logManager.Persistence** drop-down menu.
Set logging level for recovery operations. The default is trivia.	Select a logging level from the **logManager.Recovery** drop-down menu. By default, recovery logging is set to **trivia**.
Set logging level for recovery configuration operations. The default is verbose.	Select a logging level from the **logManager.RecoveryConfig** drop-down menu.
Set logging level for array-based replication operations. The default is verbose.	Select a logging level from the **logManager.Replication** drop-down menu.
Set logging level for authorization issues between Site Recovery Manager Server and vCenter Server. The default is verbose.	Select a logging level from the **logManager.ServerAuthorization** drop-down menu.
Set logging level for session management. The default is verbose.	Select a logging level from the **logManager.SessionManager** drop-down menu.
Set logging level for the SOAP Web Services adapter. The default is info.	Select a logging level from the **logManager.SoapAdapter** drop-down menu. Due to the levels of traffic that the SOAP adapter generates, setting the logging level to **trivia** might affect performance. By default, SOAP adapter logging is set to **info**.
Set logging level for storage issues. The default is verbose.	Select a logging level from the **logManager.Storage** drop-down menu.
Set logging level for messages from the array-based storage provider. The default is verbose.	Select a logging level from the **logManager.StorageProvider** drop-down menu.

5 Click **OK** to save your changes.

The new logging levels apply as soon as you click **OK**. You do not need to restart the Site Recovery Manager service. If you restart Site Recovery Manager Server, logging remains set to the level that you chose.

Change Recovery Settings

You can adjust default values for timeouts that occur when you test or run a recovery plan. You might adjust default values if tasks fail to finish because of timeouts.

Several types of timeouts can occur when recovery plan steps run. These timeouts cause the plan to pause for a specified interval to give the step time to finish.

Site Recovery Manager applies some advanced settings to a virtual machine at the moment that you configure protection on that virtual machine:

- `recovery.defaultPriority`
- `recovery.powerOnTimeout`
- `recovery.powerOnDelay`
- `recovery.customizationTimeout`
- `recovery.skipGuestShutdown`
- `recovery.powerOffTimeout`

Site Recovery Manager keeps a copy of virtual machine recovery settings on each Site Recovery Manager site. If recovery advanced settings are different on the protection and recovery sites,Site Recovery Manager initializes recovery settings for a virtual machine to different values at each site. Then when Site Recovery Manager recovers the virtual machine from site A to site B, it applies the local recovery settings for site B. When recovering from site B to site A Site Recovery Manager applies the local recovery settings for site A. This condition exists until you explicitly edit and save individual virtual machine recovery settings from the recovery plan Virtual Machines tab. Recovery settings for the affected virtual machine synchronize and become identical on both Site Recovery Manager sites.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, click **Advanced Settings**.

3 Click **Recovery**.

4 Click **Edit** to modify the recovery site settings.

Option	Action
Change the IP customization timeout. The default value is 600 seconds.	Enter a new value in the **recovery.customizationTimeout** text box.
Change the default priority for recovering a virtual machine. The default value is 3.	Enter a new value in the **recovery.defaultPriority** text box.
Enable or disable forced recovery. The default value is false.	Select or deselect the **recovery.forceRecovery** check box. Activate forced recovery in cases where a lack of connectivity to the protected site severely affects RTO. This setting only removes the restriction to select forced recovery when running a recovery plan. To actually enable forced recovery, select it when you run a plan.
Change the timeout for hosts in a cluster to power on. The default value is 1200 seconds.	Enter a new value in the **recovery.hostPowerOnTimeout** text box.
Change the timeout for guest OS to power off. The default value is 300 seconds.	Enter a new value in the **recovery.powerOffTimeout** text box. The new time-out value applies to power-off tasks for virtual machines at the protected site.

Option	Action
Change the delay after powering on a virtual machine before starting dependent tasks. The default value is 0.	Enter a new value in the **recovery.powerOnDelay** text box. The new value applies to power-on tasks for virtual machines at the recovery site.
Change the timeout to wait for VMware Tools when powering on virtual machines. The default value is 300 seconds.	Enter a new value in the **recovery.powerOnTimeout** text box. The new power-on value applies to power-on tasks for virtual machines at the recovery site. If protected virtual machines do not have VMware Tools installed, set this value to 0.
Enable or disable skipping the shutdown of the guest OS. The default value is false.	Select or deselect the **recovery.skipGuestShutdown** check box. When you select the option, recovery.powerOffTimeout has no effect. If VMware Tools are not installed in the VM, enable the option to automatically disable recovery.powerOffTimeout and shut down the SRM bypass guest and directly power off VMs without a shutdown timeout.
Enable or disable automatic VM IP customization during recovery. The default value is true.	Select or deselect the **recovery.useIpMapperAutomatically** check box. If you select the option and IP mapping rules are configured for virtual networks, then Site Recovery Manager evaluates these rules during recovery to customize the VMs. If you deselect the option, the IP mapping rules are not evaluated during recovery. You can override the option for each VM in VM Recovery Settings IP Customization mode.

5 Click **OK** to save your changes.

If you change any of these advanced settings after you have configured the protection of a virtual machine, the new settings do not apply to that virtual machine. Modifications to these advanced settings apply only to virtual machines that you protect after you changed the settings. This is by design because if Site Recovery Manager were to apply changed advanced settings to virtual machines on which you have already configured protection, this could lead to unwanted changes in the protection of those virtual machines.

What to do next

To apply the changes that you make in these advanced settings to virtual machines that you have previously protected, you must reconfigure those virtual machines individually. For example, if you reconfigure the `defaultPriority` setting, you can manually reconfigure the priority of a previously protected virtual machine to match the new `defaultPriority` setting.

1 In the vSphere Web Client, click **Site Recovery > Protection Groups**, and select the protection group to which the virtual machine belongs.

2 On the **Related Objects** tab, click **Virtual Machines**.

3 Select the virtual machine and click **Remove Protection**.

The virtual machine status changes to Not Configured.

4 Click **Configure All** to reconfigure all virtual machines in the protection group, or select a virtual machine and click **Configure Protection** to reconfigure only that virtual machine.

Site Recovery Manager applies the newer advanced settings to the virtual machine.

Change Remote Site Settings

You can modify the default values that the Site Recovery Manager Server at the protected site uses to determine whether the Site Recovery Manager Server at the remote site is available.

Site Recovery Manager monitors the connection between the protected site and the recovery site and raises alarms if the connection breaks. You can change the criteria that cause Site Recovery Manager to raise a connection event and change the way that Site Recovery Manager raises alarms.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, click **Advanced Settings**.

3 Click **Remote Site Status**.

4 Click **Edit** to modify the settings.

Option	Action
Change the number of failed pings before raising a site down event. The default value is 5.	Enter a new value in the **remoteSiteStatus.panicDelay** text box.
Change the number of remote site status checks (pings) to try before declaring the check a failure. The default value is 2.	Enter a new value in the **remoteSiteStatus.pingFailedDelay** text box.
Change the interval at which Site Recovery Manager checks whether the Site Recovery Manager Server at the remote site is available. The default value is 300 seconds.	Enter a new value in the **remoteSiteStatus.pingInterval** text box. If you specify a value for **remoteSiteStatus.pingInterval** that is less than the configured value for `connections.drPingInterval`, Site Recovery Manager resets the configured value. You can edit the `connections.drPingInterval` value in the vmware-dr.xml file. If the value specified for the **remoteSiteStatus.pingInterval** is out of range, an error message appears: `Setting for remoteSiteStatus.pingInterval is out of permitted range`.

5 Click **OK** to save your changes.

Change the Timeout for the Creation of Placeholder Virtual Machines

You can adjust replication settings to modify how long Site Recovery Manager waits for the creation of virtual machine placeholders to finish.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, click **Advanced Settings**.

3 Click **Replication**.

4 Click **Edit** to change the **replication.placeholderVmCreationTimeout** setting to modify the number of seconds to wait when creating a placeholder virtual machine.

The default value is 300.

5 Click **OK** to save your changes.

Change Storage Settings

You can adjust the storage settings to modify how Site Recovery Manager and vCenter Server communicate with the storage replication adapter (SRA).

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, click **Advanced Settings**.

3 Click **Storage**.

4 Click **Edit** to modify the storage settings.

Option	Action
Change timeout in seconds for executing an SRA command. The default value is 300 seconds.	Enter a new value in the **storage.commandTimeout** text box.
Change the maximum number of concurrent SRA operations. The default value is 5.	Enter a new value in the **storage.maxConcurrentCommandCnt** text box.
Change the minimum amount of time in seconds between datastore group computations. The default value is 0.	Enter a new value in the **storage.minDsGroupComputationInterval** text box.
Change the interval between status updates for ongoing data synchronization operations. The default value is 30 seconds.	Enter a new value in the **storage.querySyncStatusPollingInterval** text box.
Change the interval between storage array discovery checks. The default value is 86400 seconds (24 hours).	Enter a new value in the **storage.storagePingInterval** text box.
Change the maximum amount of time permitted for data synchronization operations to complete. The default value is 86400 seconds (24 hours).	Enter a new value in the **storage.syncTimeout** text box.

5 Click **OK** to save your changes.

Change Storage Provider Settings

For array-based replication, the SAN provider is the interface between Site Recovery Manager and your storage replication adapter (SRA). Some SRAs require you to change default SAN provider values. You can change the default timeout values and other behaviors of the Site Recovery Manager SAN provider.

You can change settings for resignaturing, fixing datastore names, host rescan counts, and timeouts in seconds. For more information about these values, see the SRA documentation from your array vendor.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, click **Advanced Settings**.

3 Click **Storage Provider**.

4 Click **Edit** to modify the storage provider settings.

Option	Action
Make Site Recovery Manager attempt to detach and reattach LUNs with duplicate volumes. The default value is true.	Select the **storageProvider.autoDetachLUNsWithDuplicateVolume** check box.
Set the `LVM.EnableResignature` flag on ESXi hosts during test and recovery. The default value is 0.	In the **storageProvider.autoResignatureMode** text box, enter **`0`** to disable, **`1`** to enable, or **`2`** to ignore the flag. The default setting is 0. If you set this flag to 1, Site Recovery Manager resignatures all known VMFS snapshot volumes, including any volumes that Site Recovery Manager does not manage. If you leave the flag set to 0, Site Recovery Manager only resignatures the VMFS snapshot volumes that it manages.

Option	Action
Change the timeout in seconds to wait for Batch Attach LUN operation to complete on each ESXi host. The default value is 3600 seconds.	Enter a value in the **storageProvider.batchAttachTimeoutSec** text box.
Change the timeout in seconds to wait for Batch Detach LUN operation to complete on each ESXi host. The default value is 3600 seconds.	Enter a value in the**storageProvider.batchDetachTimeoutSec** text box.
Change the interval that Site Recovery Manager waits for VMFS volumes to be mounted. The default value is 3600 seconds.	Enter a new value in the **storageProvider.batchMountTimeoutSec** text box. Change this value if you experience timeouts caused by Site Recovery Manager checking for VMFS volumes that take a long time to mount. This setting is available in Site Recovery Manager 5.5.1 and later.
Change the interval that Site Recovery Manager waits for VMFS volumes to be unmounted. The default value is 3600 seconds.	Enter a new value in the **storageProvider.batchUnmountTimeoutSec** text box. Change this value if you experience timeouts caused by Site Recovery Manager checking for VMFS volumes that take a long time to unmount. This setting is available in Site Recovery Manager 5.5.1 and later.
Force removal, upon successful completion of a recovery, of the *snap–xx* prefix applied to recovered datastore names. The default value is false.	Select the **storageProvider.fixRecoveredDatastoreNames** check box.
Delay host scans during testing and recovery. The default value is 0.	SRAs can send responses to Site Recovery Manager before a promoted storage device on the recovery site is available to the ESXi hosts. When Site Recovery Manager receives a response from an SRA, it rescans the storage devices. If the storage devices are not fully available yet, ESXi Server does not detect them and Site Recovery Manager does not find the replicated devices when it rescans. Datastores are not created and recovered virtual machines cannot be found. To delay the start of storage rescans until they are available on the ESXi hosts, enter a new value in the **storageProvider.hostRescanDelaySec** text box. Only change this value if you experience problems with unavailable datastores.
Repeat host scans during testing and recovery. The default value is 1.	Enter a new value in the **storageProvider.hostRescanRepeatCnt** text box. Some storage arrays require more than one rescan, for example to discover the snapshots of failed-over LUNs. In previous releases, you might have used the **storageProvider.hostRescanRepeatCnt** parameter to introduce a delay in recoveries. Use the **storageProvider.hostRescanDelaySec** parameter instead.
Change the interval that Site Recovery Manager waits for each HBA rescan to complete. The default value is 300 seconds.	Enter a new value in the **storageProvider.hostRescanTimeoutSec** text box.
Set the number of times that Site Recovery Manager attempts to resignature a VMFS volume. The default value is 1.	Enter a new value in the **storageProvider.resignatureFailureRetryCount** text box.
Set a timeout for resignaturing a VMFS volume. The default value is 900 seconds.	Enter a new value in the **storageProvider.resignatureTimeoutSec** text box. If you change the **storageProvider.hostRescanTimeoutSec** setting, increase the **storageProvider.resignatureTimeoutSec** setting to the same timeout that you use for **storageProvider.hostRescanTimeoutSec**.

Option	Action
Identify VMX file paths that Site Recovery Manager should not consider as potential VMX file candidates after Storage vMotion. The default value is .snapshot,	Some arrays create VMX file paths that the `storageProvider.storageVmotionVmxSearch` search algorithm should ignore. Enter a comma-separated list of strings in the **storageProvider.storageVmotionVmxFilePathsToSkip** text box to identify VMX file paths to ignore after Storage vMotion. Site Recovery Manager does not consider VMX file paths that contain one or more of these strings as potential candidate VMX files after Storage vMotion.
Search for VMX files in recovered datastores to identify virtual machines that Storage vMotion has moved before or during a test or a recovery. The default value is true.	The option is selected by default. Deselect the **storageProvider.storageVmotionVmxSearch** check box to disable this option.
Set the timeout in seconds for batch unmount datastore operations. The default value is 3600 seconds.	Enter the value in the **storageProvider.batchUnmountTimeoutSec** text box.
Set number of retries for batch unmount of VMFS/NFS volumes. The default value is 3.	Enter the new value in the **storageProvider.datastoreUnmountRetryCnt** text box.
Set the timeout in seconds to wait for the Virtual Center to report newly discovered datastores. The default value is 30 seconds.	Enter the new value in the **storageProvider.waitForRecoveredDatastoreTimeoutSec** text box.
Set the timeout in seconds to wait for newly discovered datastores to become accessible. The default value is 60 seconds.	Enter the new value in the **storageProvider.waitForAccessibleDatastoreTimeoutSec** text box.
Set the time interval in seconds that Site Recovery Manager waits for VMFS volumes to become mounted. The default value is 30 seconds.	Enter the new value in the **storageProvider.waitForVmfsVolumesMountedStateTimeoutSec** text box.

5 Click **OK** to save your changes.

Change vSphere Replication Settings

You can adjust global settings to change how Site Recovery Manager interacts with vSphere Replication.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, click **Advanced Settings**.

3 Click **vSphere Replication**.

4 Click **Edit** to modify the vSphere Replication settings.

Option	Description
Allow vSphere Replication to recover virtual machines that are included in Site Recovery Manager recovery plans independently of Site Recovery Manager. The default value is false.	If you configure vSphere Replication on a virtual machine and include the virtual machine in a Site Recovery Manager recovery plan, you cannot recover the virtual machine by using vSphere Replication independently of Site Recovery Manager. To allow vSphere Replication to recover virtual machines independently of Site Recovery Manager, select the **allowOtherSolutionTagInRecovery** check box.
Keep older multiple point in time (PIT) snapshots during recovery. The default value is true.	If you configure vSphere Replication to take PIT snapshots of protected virtual machines, Site Recovery Manager only recovers the most recent snapshot when you perform a recovery. To recover older PIT snapshots during recovery, select the **preserveMpitImagesAsSnapshots** check box.

Option	Description
Change the timeout period for reverse replication during reprotect operations. The default value is 3600.	Enter a new value in the **reverseReplicationTimeout** text box. Change this value if you experience timeout errors when vSphere Replication reverses replication during reprotect operations.
Change the timeout period for vSphere Replication synchronization operations. The default value is 7200.	Enter a new value in the **synchronizationTimeout** text box. Change this value if you experience timeout errors when vSphere Replication synchronizes virtual machines on the recovery site.
Change the default RPO setting for replications. The default value is 240.	Enter a new value in the **vrReplication.timeDefault** text box. The default value is 240 minutes (4 hours). This value is selected when you configure replications, but you can specify a different RPO in the Configure Replication wizard when you configure replication for an individual virtual machine or for a group of virtual machines.

5 Click **OK** to save your changes.

Modify Settings to Run Large Site Recovery Manager Environments

If you use Site Recovery Manager to test or recover a large number of virtual machines, you might need to modify the default Site Recovery Manager settings to achieve the best possible recovery times in your environment or to avoid timeouts.

In large environments, Site Recovery Manager might simultaneously power on or power off large numbers of virtual machines. Simultaneously powering on or powering off large numbers of virtual machines can create a heavy load on the virtual infrastructure, which might lead to timeouts. You can modify certain Site Recovery Manager settings to avoid timeouts, either by limiting the number of power on or power off operations that Site Recovery Manager performs concurrently, or by increasing the timeout periods.

The limits that you set on power on or power off operations depend on how many concurrent power on or power off operations your infrastructure can handle.

You modify certain options in the **Advanced Settings** menus in the vSphere Web Client or in the Site Recovery Manager client plug-in. To modify other settings, you edit the `vmware-dr.xml` configuration file on the Site Recovery Manager Server. Always modify settings by using the client menus when an option exists. If you modify settings, you must make the same modifications on the Site Recovery Manager Server and vCenter Server instances on both the protected and recovery sites.

For descriptions of the settings that you can change, see "Settings for Large Site Recovery Manager Environments," on page 112.

Procedure

1 In the vSphere Web Client, select a cluster.

2 On the **Manage** tab, select **Settings > vSphere DRS**.

3 Click **Edit**.

4 In **Advanced Options**, set the `srmMaxBootShutdownOps` setting.

Option	Description
Option text box	Enter `srmMaxBootShutdownOps`.
Value text box	Enter the maximum number of boot shutdown operations, for example 32.

5 Click **OK** to save your changes.

6 Log in to the Site Recovery Manager Server host.

7 Open the `vmware-dr.xml` file in a text editor.

You find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder.

8 Change the `defaultMaxBootAndShutdownOpsPerCluster` and `defaultMaxBootAndShutdownOpsPerHost` settings in the `vmware-dr.xml` file:

```
<config>
...
   <defaultMaxBootAndShutdownOpsPerCluster>24</defaultMaxBootAndShutdownOpsPerCluster>
   <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
...
</config>
```

9 Restart the Site Recovery Manager Server to apply the new settings.

10 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

11 Select **vSphere Replication** and increase the `vrReplication.synchronizationTimeout` setting.

The default value is 7200 seconds.

12 Select **Storage** and increase the `storage.commandTimeout` setting.

The default value is 300 seconds.

13 Click **OK** to save your changes.

Settings for Large Site Recovery Manager Environments

To protect a large number of virtual machines, you can modify the default Site Recovery Manager settings to achieve the best possible recovery times in your environment or to avoid timeouts.

You modify certain options in the **Advanced Settings** menus in the vSphere Web Client or in the Site Recovery Manager client plug-in. To modify other settings, you edit the `vmware-dr.xml` configuration file on the Site Recovery Manager Server. Always modify settings by using the client menus when an option exists. If you modify settings, you must make the same modifications on the Site Recovery Manager Server and vCenter Server instances on both the protected and recovery sites.

To modify the settings, see "Modify Settings to Run Large Site Recovery Manager Environments," on page 111.

Table 10-1. Settings that Modify the Number of Simultaneous Power On or Power Off Operations

Option	Description
srmMaxBootShutdownOps	Specifies the maximum number of concurrent power-on operations for any given cluster. Guest shutdowns, but not forced power offs, are throttled according to this value. Guest shutdowns occur during primary site shutdowns (planned failover) and IP customization workflows. Modify this option per cluster in the vSphere Web Client by right-clicking a cluster and selecting **Settings**. Click **vSphere DRS**, then **Edit > Advanced Options**. Type the option to override the **defaultMaxBootAndShutdownOpsPerCluster** value that you can set in the `vmware-dr.xml` file. You can set a global value **defaultMaxBootAndShutdownOpsPerCluster** in the `vmware-dr.xml` file, and then set different **srmMaxBootShutdownOps** values for individual clusters in the vSphere Web Client. By default, throttling is turned off.
defaultMaxBootAndShutdownOpsPerCluster	Specifies the maximum number of concurrent power-on operations for all clusters that Site Recovery Manager protects. Guest shutdowns, but not forced power offs, are throttled according to this value. Guest shutdowns occur during primary site shutdowns (planned failover) and IP customization workflows. You modify this setting in the `vmware-dr.xml` file. The **srmMaxBootShutdownOps** value that you can set in the vSphere Web Client overrides the **defaultMaxBootAndShutdownOpsPerCluster** value. You can set a global value **defaultMaxBootAndShutdownOpsPerCluster** in the `vmware-dr.xml` file, and then set different **srmMaxBootShutdownOps** values for individual clusters in the vSphere Web Client. By default, throttling is turned off.
defaultMaxBootAndShutdownOpsPerHost	Specifies the maximum number of concurrent power-on operations on any standalone host. You can only set the option in the `vmware-dr.xml` file. By default, throttling is turned off.

Table 10-2. Settings that Modify Timeout Periods

Option	Description
vrReplication.synchronizationTimeout	Site Recovery Manager enforces a timeout to complete an online or offline synchronization for virtual machines replicated by vSphere Replication during a test or failover. If a synchronization does not finish within the given timeout, for example, because of a slow network or a large virtual machine, Site Recovery Manager reports a failure during a test or failover. Modify this option in the vSphere Web Client. In **Site Recovery**, select a site. On the **Manage** tab, select **Advanced Settings > vSphere Replication**. The default value is 7200 seconds.
storage.commandTimeout	The timeout for running SRA commands in ABR-related workflows. In some cases, such as surfacing LUNs and snapshots, some arrays take longer than the default time to respond. Modify this option in the vSphere Web Client. In **Site Recovery**, select a site. On the **Manage** tab, select**Advanced Settings > Storage**. The default value is 300 seconds.

Modify Settings for Long-Running Tasks

If you run tasks that take a long time to complete, the default timeout period on the remote site might elapse before the task completes. You can configure additional timeouts to allow long-running tasks to finish.

A long-running task might be the test recovery or cleanup of a large virtual machine. If a virtual machine has large disks, it can take a long time to perform a test recovery or to perform a full recovery. The default timeout period monitors the connectivity between the sites, so if a task takes a longer time to complete than the default timeout period and does not send notifications to the other site while it is running, timeouts can result. In this case, you can add a setting in the `vmware-dr.xml` configuration file so that Site Recovery Manager does not timeout before a long-running task finishes.

By adding the `<RemoteManager><TaskDefaultTimeout>` setting to `vmware-dr.xml`, you configure an additional timeout period for tasks to finish on the remote site. You can also configure a `<TaskProgressDefaultTimeout>` setting, to extend the time that Site Recovery Manager gives to a task if it reports its progress at regular intervals.

If you configure a `<TaskDefaultTimeout>` period, the default timeout does not cause tasks to fail, even if they take longer to complete than the period that the `<DefaultTimeout>` setting defines. As long as Site Recovery Manager continues to receive task progress notifications from the remote site, long-running tasks such as test recovery or cleanup of large virtual machines do not time out.

The initial call to start a task is subject to the `<DefaultTimeout>` setting. After they start, long-running tasks are subject to the `<TaskDefaultTimeout>` setting. If a task has not finished when `<TaskDefaultTimeout>` expires, the progress monitor checks whether the task has sent any progress notifications. If the task has sent notifications, the progress monitor applies the `<TaskProgressDefaultTimeout>` setting to allow the task more time to finish. When `<TaskProgressDefaultTimeout>` expires, the progress monitor checks for progress notifications again. If the task has sent progress notifications, the progress monitor gives the task more time. The sequence repeats until the task finishes or until it stops sending progress notifications.

Procedure

1 Log in to the Site Recovery Manager Server host.

2 Open the `vmware-dr.xml` file in a text editor.

You find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder.

3 Locate the `<RemoteManager>` element in the `vmware-dr.xml` file.

The default timeout for startign all tasks on the remote site is 900 seconds, or 15 minutes.

```
<RemoteManager>
 <DefaultTimeout>900</DefaultTimeout>
</RemoteManager>
```

4 Add a `<TaskDefaultTimeout>` element inside the `<RemoteManager>` tags.

Set the `<TaskDefaultTimeout>` period to a number of seconds that is greater than the `<DefaultTimeout>` period. `<TaskDefaultTimeout>` has no maximum limit.

```
<RemoteManager>
 <DefaultTimeout>900</DefaultTimeout>
 <TaskDefaultTimeout>2700</TaskDefaultTimeout>
</RemoteManager>
```

5 Add a <TaskProgressDefaultTimeout> element inside the <RemoteManager> tags.

The <TaskProgressDefaultTimeout> must be at least 1/100th of the <TaskDefaultTimeout> period. If you set a period that is less than 1/100th of the <TaskDefaultTimeout> period, Site Recovery Manager silently adjusts the timeout.

```
<RemoteManager>
 <DefaultTimeout>900</DefaultTimeout>
 <TaskDefaultTimeout>2700</TaskDefaultTimeout>
 <TaskProgressDefaultTimeout>27</TaskProgressDefaultTimeout>
</RemoteManager>
```

6 Save and close the vmware-dr.xml file.

7 Restart the Site Recovery Manager Server service to apply the new settings.

Site Recovery Manager Events and Alarms

11

Site Recovery Manager supports event logging. Each event includes a corresponding alarm that Site Recovery Manager can trigger if the event occurs. This provides a way to track the health of your system and to resolve potential issues before they affect the protection that Site Recovery Manager provides.

This chapter includes the following topics:

How Site Recovery Manager Monitors Connections Between Sites

Site Recovery Manager monitors the connection between the protected and recovery sites and logs events if the remote site stops responding.

When Site Recovery Manager establishes the connection between two paired Site Recovery Manager Server instances, the Site Recovery Manager Server that initiated the connection sends a `RemoteSiteUpEvent`.

If Site Recovery Manager detects that a monitored connection has broken, it starts periodic connection checks by sending a `ping` request to the remote site. Site Recovery Manager monitors the connection checks and logs events.

- Site Recovery Manager sends pings at regular intervals. You can configure this interval by setting the `remoteSiteStatus.pingInterval` value. The default is 300 seconds.
- The connection monitor skips a number of failed pings. You can configure this number by setting the `remoteSiteStatus.pingFailedDelay` value. The default is 2.
- When the number of skipped failed pings exceeds the value of the `remoteSiteStatus.pingFailedDelay` setting, Site Recovery Manager sends a `RemoteSitePingFailedEvent` event.
- When the number of skipped failed pings exceeds a higher limit Site Recovery Manager sends a `RemoteSiteDownEvent` event for every failed ping and stops sending `RemoteSitePingFailedEvent` events. You can configure this higher limit of failed pings by setting the `remoteSiteStatus.panicDelay` setting. The default is 5.
- Site Recovery Manager continues to send `RemoteSiteDownEvent` events until the connection is reestablished.
- When a connection to the remote site Site Recovery Manager Server is reestablished, Site Recovery Manager sends `RemoteSiteUpEvent` events.

Configure Site Recovery Manager Alarms

Site Recovery Manager adds alarms to the alarms that vCenter Server supports. You can configure Site Recovery Manager alarms to send an email notification, send an SNMP trap, or to run a script on the vCenter Server host.

The **Alarm Definitions** tab in the **Manage** of the vSphere Web Client lists all of the Site Recovery Manager alarms. You can edit the settings for each alarm to specify the action for Site Recovery Manager to take when an event triggers the alarm. By default, none of the Site Recovery Manager alarms act until you configure the alarm.

NOTE In an environment with more than one vCenter Server, Site Recovery Manager displays all events from the Site Recovery Manager Servers that are registered as extensions, even if you select events for a specific vCenter Server.

Prerequisites

For alarms to send email notifications, configure the **Mail** settings in the **vCenter Server Settings** menu. See *ESXi and vCenter Server Documentation*.

Procedure

1 In the vSphere Web Client, click a vCenter Server

2 In the **Manage** tab, click **Alarm Definitions** tab to display the list of vCenter Server alarms.

3 Click **Add** to add a new alarm.

4 On the **General** page, enter an alarm name, description, and select the object you want to monitor from the drop-down list.

5 Choose a specific event that occurs on the object.

6 Select the **Enable this alarm** check box to enable the action for this alarm, and click **Next**.

7 On the **Triggers** page, click **Add** to add an event trigger.

8 Select an event from the drop-down list and the corresponding status.

   If you see repeated events in the list, each event represents a single Site Recovery Manager instance and triggers an alarm for the extension with which it is registered. For example, in a scenario with multiple Site Recovery Manager instances, you can use `RecoveryPlanCreated (SRM 1)` and `RecoveryPlanCreated (SRM 2)` for the same event on both extensions.

9 To add a condition that triggers the alarm, click **Add**, select an argument from the drop-down list, the operator, and the transition from warning to critical condition.

10 Click **Next**.

11 On the **Actions** page, select an action from the drop-down list, enter the relevant information in the configuration column, when to run the action, the number of minutes to repeat the action, and click **Finish**.

What to do next

To edit an alarm definition, right-click an alarm and select **Edit**.

Site Recovery Manager Events Reference

Site Recovery Manager monitors different types of events.

Site Status Events

Site status events provide information about the status of the protected and recovery sites and the connection between them.

Table 11-1. Site Status Events

Event	Description	Cause
`UnknownStatusEvent`	Unknown status	Site Recovery Manager Server status is not available
`RemoteSiteDownEvent`	Remote site down	Site Recovery Manager Server has lost its connection with the remote Site Recovery Manager Server.
`RemoteSitePingFailedEvent`	Remote site ping failed	Failures at the remote site or network connectivity problems.
`RemoteSiteCreatedEvent`	Remote site created	Local site has been successfully paired with the remote site.
`RemoteSiteUpEvent`	Remote site up	Site Recovery Manager Server re-establishes its connection with the remote Site Recovery Manager Server.
`RemoteSiteDeletedEvent`	Remote site deleted	Remote Site Recovery Manager site has been deleted.
`HbrGroupVmAssociatedEvent`	vSphere Replication replicated virtual machine is added to a protection group	A virtual machine replicated by vSphere Replication is added to a protection group.
`HbrGroupVmDisassociatedEvent`	vSphere Replication replicated virtual machine is removed from a protection group	A virtual machine replicated by vSphere Replication is removed from a protection group.
`LocalHmsConnectionDownEvent`	Local vSphere Replication Server is down	Repeated connection attempts to vSphere Replication fail.
`LocalHmsConnectionUpEvent`	The connection to the local vSphere Replication Server has been restored	Connection to vSphere Replication is successful.
`LocalHmsPingFailedEvent`	The local vSphere Replication Server is not responding	Failure to establish connection to the local vSphere Replication Server
`LocalQsConnectionDownEvent`	The local inventory service is down	Unable to connect to the local inventory service server. You can specify the number of internal pings to skip before Site Recovery Manager throws `LocalQsConnectionDownEvent` by adding `<connections><qsPanicDelay>`*`integer`*`</qsPanicDelay></connections>` in the `vmware-dr.xml` configuration file.

Table 11-1. Site Status Events (Continued)

Event	Description	Cause
LocalQsConnectionUpEvent	The connection to the local inventory service is restored	Connection to the local inventory server is successful. You can specify the interval between pings from Site Recovery Manager to the inventory service by adding <connections><qsPingInterval>*number of seconds*</qsPingInterval></connections> in the vmware-dr.xml configuration file.
LocalQsPingFailedEvent	The local inventory service is not responding	Connection attempt to the local inventory service fails. You can specify the number of internal pings to skip before Site Recovery Manager throws LocalQsPingFailedEvent by adding <connections><qsPingFailedDelay>*integer*</qsPingFailedDelay></connections> in the vmware-dr.xml configuration file.
LowDiskSpaceEvent	Low disk space	Free disk space on the local site is low.
LowMemoryEvent	Low memory	Available memory on the local site is low.

Protection Group Events

Protection Group events provide information about actions and status related to protection groups.

These events have three categories:

- Protection Group Replication Informational Events
- Protection Group Replication Warning Events
- Protection Group Replication Error Events

Table 11-2. Protection Group Replication Informational Events

Event	Description	Cause
CreatedEvent	Created protection group.	Posted on both vCenter Servers in the completion of the Commit phase of creating a protection group.
RemovedEvent	Removed protection group.	Posted on both vCenter Servers in the completion of the Commit phase of removing a protection group.
ReconfiguredEvent	Reconfigured protection group.	Posted on both vCenter Servers in the completion of the Commit phase of reconfiguring a protection group.
ProtectedVmCreatedEvent	Virtual machine in group is configured for protection.	Posted on both vCenter Servers in the completion of the Commit phase of the protection of a virtual machine.
ProtectedVmRemovedEvent	Virtual machine in group is no longer configured for protection.	Posted on both vCenter Servers in the completion of the Commit phase of unprotecting a virtual machine.
ProtectedVmReconfiguredProtectionSettingsEvent	Reconfigured protection settings for virtual machine.	Posted on both vCenter Servers in the completion of the Commit phase of reconfiguring virtual machine protection settings.

Table 11-2. Protection Group Replication Informational Events (Continued)

Event	Description	Cause
ProtectedVmReconfiguredRecoveryLocationSettingsEvent	Reconfigured recovery location settings for virtual machine.	Posted on the protected site vCenter Server only on the successful completion of reconfiguring the recovery location settings for a protected virtual machine.
PlaceholderVmCreatedEvent	The placeholder virtual machine was created in the vCenter Serverinventory.	Posted on the recovery site vCenter Server placeholder virtual machine is created as a result of protection, repair operation. .
PlaceholderVmCreatedFromOldProductionVmEvent	The placeholder virtual machine was created in the vCenter Server inventory using the identity of the old protected virtual machine.	Posted on the recovery site vCenter Server placeholder virtual machine is created as a result of swapping the old protected virtual machine with a placeholder virtual machine during or after reprotect operation .

Table 11-3. Protection Group Replication Warning Events

Event	Description	Cause
VmFullyProtectedEvent	Virtual machine in group: Unresolved devices have all been resolved.	A protected virtual machine's previously unresolved devices have all been resolved.
VmNotFullyProtectedEvent	Virtual machine in group: One or more devices need to be configured for protection.	Posted on the protected site vCenter Server only upon device handling updating the recovery location settings with a non-empty unresolvedDevices set. This can be triggered by changes to the protected virtual machine or during reprotect of a virtual machine.
PlaceholderVmUnexpectedlyDeletedEvent	Virtual machine in group: The placeholder virtual machine was removed from the vCenter Server inventory.	Posted on the recovery site vCenter Server when Site Recovery Manager detects that the placeholder virtual machine was unexpectedly deleted or removed from the vCenter Server inventory.

Table 11-4. Protection Group Replication Error Events

Event	Description	Cause
ProductionVmDeletedEvent	Virtual machine in group: The protected virtual machine has been removed from the virtual machineware vCenter Server inventory.	Posted when a protected virtual machine is deleted or removed from the vCenter Server inventory.
ProductionVmInvalidEvent	Virtual machine in group: Cannot resolve the file locations of the protected virtual machine for replication.	Posted when the replication provider cannot find the protected virtual machine files in order to replicate them.

Recovery Events

Recovery events provide information about actions and status related to the Site Recovery Manager recovery processes.

Table 11-5. Recovery Events

Event	Description	Cause
`RecoveryVmBegin`	Recovery plan has begun recovering the specified virtual machine.	Signaled when the recovery virtual machine was successfully created. If some error occurred before the virtual machine ID is known the event is not fired.
`RecoveryVmEnd`	Recovery plan has completed recovering the virtual machine.	Signaled after the last post-power on script has completed, or after a recovery-stopping error has occurred for the virtual machine.
`PlanCreated`	Recovery plan *hostname*has been created.	Signaled when a new plan is created. It is sent to each vCenter Server instance where the plan is hosted.
`PlanDestroy`	Recovery plan has been destroyed.	Signaled when a plan has been deleted from the site. Note that on the site where the plan has been requested to deleted there can be a significant delay, while it waits for the plan to be deleted at the other site. It will be sent to each vCenter Server instance where the plan is hosted.
`PlanEdit`	Recovery plan was changed.	Signaled when an existing plan is edited.
`PlanExecTestBegin`	Recovery plan has begun a test.	Signaled on the recovery site when a recovery test is initiated.
`PlanExecTestEnd`	Recovery plan has completed a test.	Signaled on the recovery site when a recovery test has completed.
`PlanExecCleanupBegin`	Recovery plan has begun a test cleanup.	Signaled on the recovery site when a test cleanup is initiated.
`PlanExecCleanupEnd`	Recovery plan has completed a test cleanup.	Signaled on the recovery site when a test cleanup has completed.
`PlanExecBegin`	Recovery plan has begun a recovery.	Signaled on the recovery site when a recovery is initiated.
`PlanExecEnd`	Recovery plan has completed a recovery.	Signaled on the recovery site when a recovery has completed.
`PlanExecReprotectBegin`	Recovery plan has begun a reprotect operation.	Signaled on the recovery site when a reprotect is initiated.
`PlanExecReprotectEnd`	Recovery plan has completed a reprotect operation.	Signaled on the recovery site when a reprotect has completed.
`PlanPromptDisplay`	Recovery plan is displaying a prompt and is waiting for user input.	Signaled on the recovery site when a prompt step is encountered. The key is a unique identifier for the prompt.
`PlanPromptResponse`	Recovery plan has received an answer to its prompt.	Signaled on the recovery site when a prompt step is closed.

Table 11-5. Recovery Events (Continued)

Event	Description	Cause
PlanServerCommandBegin	Recovery plan has started to run a command on the Site Recovery Manager Server machine.	Signaled on the recovery site when Site Recovery Manager has started to run a callout command on the Site Recovery Manager Server machine.
PlanServerCommandEnd	Recovery plan has completed executing a command on the Site Recovery Manager Server machine.	Signaled on the recovery site when Site Recovery Manager has finished running a callout command on the Site Recovery Manager Server machine.
PlanVmCommandBegin	Recovery plan has started to run a command on a recovered virtual machine.	Signaled on the recovery site when Site Recovery Manager has started to run a callout command on a recovered virtual machine.
PlanVmCommandEnd	Recovery plan has completed executing a command on a recovered virtual machine.	Signaled on the recovery site when Site Recovery Manager has finished running a callout command on a recovered virtual machine.

Storage and Storage Provider Events

Storage and storage provider events provide information about actions and status related storage or storage providers.

Table 11-6. SRA Events

Event	Description	Cause
StorageAdaptLoadEvent	Loaded the specified SRA.	Site Recovery Manager detected new SRA either during startup or during user-initiated SRAs reload.
StorageAdaptReloadFailEvent	Failed to load SRA from the specified path.	Site Recovery Manager failed to reload previously known SRA either during startup or during user-initiated SRAs reload.
StorageAdaptChangeEvent	Loaded new version of the specified SRA.	Site Recovery Manager detected that previously known SRA was upgraded.

Table 11-7. Array Manager Events

Event	Description	Cause
SAManagerAddedEvent	Created the specified array manager using the specified SRA.	User added an Array Manager.
SAManagerRemovedEvent	Deleted the specified array manager.	User removed an Array Manager.
SAManagerReconfigEvent	Reconfigured the specified array manager.	User edited Array Manager properties.
SAManagerPingOkEvent	Ping for the specified array manager succeeded.	Site Recovery Manager Server successfully pinged an Array Manager.
SAManagerPingFailEvent	Failed to ping the specified array manager.	An error occurred during Array Manager ping.

Table 11-8. Array Pair Events

Event	Description	Cause
SAPairDiscoveredEvent	Discovered replicated array pair with Array Manager.	User created Array Manager which discovered replicated array pairs.
SAPairEnabledEvent	Enabled replicated array pair with Array Manager.	User enabled an Array Pair.
SAPairDisabledEvent	Disabled replicated array pair with Array Manager.	User disabled an Array Pair.
SAPairPingOkEvent	Ping for replicated array pair succeeded.	Site Recovery Manager Server successfully pinged the array pair.
SAPairPingFailEvent	Failed to ping replicated array pair.	An error occurred during Array Pair ping.

Table 11-9. Datastore Events

Event	Description	Cause
StorageDsDiscoveredEvent	Discovered replicated datastore.	Site Recovery Manager Server discovered replicated datastore.
StorageDsLostEvent	Specified datastore is no longer replicated.	User turned off replication of storage devices backing the datastore.
StorageRdmDiscoveredEvent	Discovered replicated RDM attached to specified virtual machine.	Site Recovery Manager Server discovered replicated RDM. This is raised when you add an RDM disk to a protected virtual machine.
StorageRdmLostEvent	RDM attached to specified virtual machine is no longer replicated.	User turned off replication of the LUN backing the RDM.

Table 11-10. Protection Events

Event	Description	Cause
SPDsProtEvent	Protected datastore in specified protection group.	User included datastore in new or existing protection group.
SPDsUnprotEvent	Unprotected specified datastore.	User removed datastore from protection group or deleted protection group which contained this datastore. This is raised if you unprotect a datastore either by removing it from a protection group or by removing the protection group.
SPVmDiscoveredEvent	Discovered replicated virtual machine.	User created virtual machine on a replicated datastore.
SPVmLostEvent	Specified virtual machine is no longer replicated	User migrated virtual machine off of the replicated datastore.
SPDsProtMissingEvent	Replicated datastore needs to be included in specified protection group but is included in an alternate protection group.	This is raised if you have a datastore that needs to be merged and is still not protected. At the conflict event, the datastore is already protected.
SPDsProtConflictEvent	Replicated datastore needs to be included in specified protection group.	This is raised if you have a datastore that needs to be merged and is still not protected. At the conflict event, the datastore is already protected.
SPDsReplicationLostEvent	Datastore included in specified protection group is no longer replicated.	User turned off replication for devices backing the datastore.

Table 11-10. Protection Events (Continued)

Event	Description	Cause
SPGroupProtRestoredEvent	Protection has been restored for specified protection group.	The previous (non-empty) issues of a protection group are cleared.
SPVmDsProtMissingEvent	Datastore used by virtual machine needs to be included in specified protection group.	If you add a datastore to a VM that is already protected by a protection group and this datastore is not part of this protection group, you need to add it.
SPVmDsProtConflictEvent	Datastore used by specified virtual machine needs to be added to specified protection group, but is currently in use by an alternate protection group.	If you add a datastore to a VM that is already protected by a protection group and this datastore is not part of this protection group, you need to add it.
SPVmDsReplicationLostEvent	Datastore used by specified virtual machine and included in specified protection group is no longer replicated.	See description.
SPVmProtRestoredEvent	Protection for specified virtual machine in specified protection group has been restored.	The previous (non-empty) issues for a protected virtual machine are cleared. The event will not be posted when issues related to non-protected virtual machine are cleared
SPCgSpansProtGroupsEvent	Specified consistency group spans specified protection groups.	This is raised if you have two datastores protected in different protection groups but then later you merge them into a single consistency group on the array.
SPCgDsMissingProtEvent	Datastore from specified consistency group needs to be included in specified protection group.	See description.
SPDsSpansConsistGroupsEvent	Datastore spans devices from different consistency groups.	This is raised if you have a datastore on top of multiple LUNs but these LUNs do not belong to the same consistency group.
SPNfsDsUrlConflictEvent	NFS datastores mounted from specified volume have different URLs mounted from the remote host. The remote path has the specified URL, while the datastore mounted from the other host has the specified URL.	The same NFS volume is mounted using the different IP addresses of the same NFS server in two different datastores.

Licensing Events

Licensing events provide information about changes in Site Recovery Manager licensing status.

Table 11-11. Licensing Events

Event	Description	Cause
`LicenseExpiringEvent`	The Site Recovery Manager License at the specified site expires in the specified number of days.	Every 24 hours, non-evaluation, expiring licenses are checked for the number of days left. This event is posted with the results.
`EvaluationLicenseExpiringEvent`	The Site Recovery Manager Evaluation License at the specified site expires in the specified number of days.	Every 24 hours, evaluation licenses are checked for the number of days left. This event is posted with the results.
`LicenseExpiredEvent`	The Site Recovery Manager license at the specified site license has expired.	Every 30 minutes, expired (non-evaluation) licenses will post this event.
`EvaluationLicenseExpiredEvent`	The Site Recovery Manager Evaluation License at the specified site license has expired.	Every 30 minutes, evaluation licenses will post this event.
`UnlicensedFeatureEvent`	The Site Recovery Manager license at the specified site is overallocated by the specified number of licenses.	Every 24 hours and upon the protection or unprotection of a virtual machine, this event will be posted if the total number of licenses exceeds the capacity in the license.
`LicenseUsageChangedEvent`	The Site Recovery Manager license at the specified site is using the specified number out of the total number licenses.	Every 24 hours and upon the protection or unprotection of a virtual machine, this event will be posted if the total number of licenses does not exceed the capacity in the license.

Permissions Events

Permission events provide information about changes to Site Recovery Manager permissions.

Table 11-12. Permissions Events

Event	Description	Cause
`PermissionsAddedEvent`	Permission created for the entity on Site Recovery Manager.	A permission for the entity was created using the role specified. The `IsPropagate` flag indicates whether the permission is propagated down the entity hierarchy.
`PermissionsDeletedEvent`	Permission rule removed for the entity on Site Recovery Manager.	A permission for the entity was deleted.
`PermissionsUpdatedEvent`	Permission changed for the entity on Site Recovery Manager.	A permission for the indicated entity was modified.

SNMP Traps

Site Recovery Manager sends SNMP traps to community targets defined in vCenter Server. You can configure them using the vSphere Web Client. When you enter localhost or 127.0.0.1 as a target host for SNMP traps, Site Recovery Manager uses the IP address or host name of the vSphere server as configured by the Site Recovery Manager installer.

SNMP traps for Site Recovery Manager 5.x are backward compatible with Site Recovery Manager 4.0 and later releases.

Table 11-13. SNMP Traps

Event	Description	Cause
`RecoveryPlanExecuteTestBeginTrap`	This trap is sent when a recovery plan starts a test.	Site Recovery Manager site name, recovery plan name, recovery type, execution state.
`RecoveryPlanExecuteTestEndTrap`	This trap is sent when a recovery plan ends a test.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, result status.
`RecoveryPlanExecuteCleanupBeginTrap`	This trap is sent when a recovery plan starts a test cleanup.	Site Recovery Manager site name, recovery plan name, recovery type, execution state.
`RecoveryPlanExecuteCleanupEndTrap`	This trap is sent a recovery plan ends a test cleanup.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, result status.
`RecoveryPlanExecuteBeginTrap`	This trap is sent when a recovery plan starts a recovery.	Site Recovery Manager site name, recovery plan name, recovery type, execution state.
`RecoveryPlanExecuteEndTrap`	This trap is sent when a recovery plan ends a recovery.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, result status.
`RecoveryPlanExecuteReprotectBeginTrap`	This trap is sent when Site Recovery Manager starts the reprotect workflow for a recovery plan.	Site Recovery Manager site name, recovery plan name, recovery type, execution state.
`RecoveryPlanExecuteReprotectEndTrap`	This trap is sent when Site Recovery Manager has finished the reprotect workflow for a recovery plan.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, result status.
`RecoveryVmBeginTrap`	This trap is sent when a recovery plan starts recovering a virtual machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, virtual machine name, virtual machine UUID.
`RecoveryVmEndTrap`	This trap is sent when a recovery plan has finished recovering a virtual machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, virtual machine name, virtual machine UUID, result status.
`RecoveryPlanServerCommandBeginTrap`	This trap is sent when a recovery plan starts the execution of a command callout on Site Recovery Manager Server machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, command name.
`RecoveryPlanServerCommandEndTrap`	This trap is sent when a recovery plan has finished the execution of a command callout on Site Recovery Manager Server machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, command name, result status.

Table 11-13. SNMP Traps (Continued)

Event	Description	Cause
`RecoveryPlanVmCommandBeginTrap`	This trap is sent when a recovery plan starts the execution of a command callout on a recovered virtual machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, command name, virtual machine name, virtual machine UUID.
`RecoveryPlanVmCommandEndTrap`	This trap is sent when a recovery plan has finished the execution of a command callout on a recovered virtual machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, command name, virtual machine name, virtual machine UUID, result status.
`RecoveryPlanPromptDisplayTrap`	This trap is sent when a recovery plan requires user input before continuing.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, prompt string.
`RecoveryPlanPromptResponseTrap`	This trap is sent when a recovery plan no longer requires user input before continuing.	Site Recovery Manager site name, recovery plan name, recovery type, and execution state.

Collecting Site Recovery Manager Log Files

12

To help identify the cause of any problems you encounter during the day-to-day running of Site Recovery Manager, you might need to collect Site Recovery Manager log files to review or send to VMware Support.

Site Recovery Manager creates several log files that contain information that can help VMware Support diagnose problems. You can use the Site Recovery Manager log collector to simplify log file collection.

The Site Recovery Manager Server and client use different log files.

The Site Recovery Manager Server log files contain information about the server configuration and messages related to server operations. The Site Recovery Manager Server log bundle also contains system information and history reports of the latest recovery plan executions.

The Site Recovery Manager client log files contain information about the client configuration and messages related to client plug-in operations. The Site Recovery Manager bundle also includes installer log files and the contents of the storage replication adapters (SRA) subdirectory of the log directory.

Log files from vCenter Server instances and ESXi Server instances that are part of your Site Recovery Manager system might also include information useful for diagnosing Site Recovery Manager problems.

The Site Recovery Manager log file collects or retrieves the files and compresses them in a zipped file that is placed in a location that you choose.

Errors that you encounter during Site Recovery Manager operations appear in error dialog boxes or appear in the Recent Tasks window. Most errors also generate an entry in a Site Recovery Manager log file. Check the recent tasks and log files for the recovery site and the protected site.

This chapter includes the following topics:

Collect Site Recovery Manager Log Files By Using the Site Recovery Manager Interface

You can download logs for Site Recovery Manager to a user-specified location.

Use this information to understand and resolve issues. For best results, collect logs from each site.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 From the **Actions** menu, and select **Export SRM Log**. You can also right-click the site and select **Export SRM Log**.

3 In the **Export SRM Log** wizard, click **Generate Log** and wait for the operation to complete.

4 Click **Download Log** to download the logs.

Collect Site Recovery Manager Log Files Manually

You can download Site Recovery Manager Server log files in a log bundle that you generate manually. This is useful if you are unable to access the vSphere Client.

The bundle of logs that these procedures generate is identical to the logs that you generate by using the vSphere Client.

Procedure

- Initiate the collection of Site Recovery Manager Server log files from the **Start** menu:
  a Log in to the Site Recovery Manager Server host.
  b Select **Start > Programs > VMware > VMware Site Recovery Manager > Generate VMware vCenter Site Recovery Manager log bundle**.
- Initiate the collection of Site Recovery Manager Server log files from the Windows command line:
  a Start a Windows command shell on the Site Recovery Manager Server host.
  b Change directory to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`.
  c Run the following command.

```
cscript srm-support.wsf
```

The individual log files are collected in a file named `srm-support-MM-DD-YYYY-HH-MM.zip`, where *MM-DD-YYYY-HH-MM* indicates the month, day, year, hour, and minute when the log files were created. The log bundle is saved on the desktop by default.

Change Size and Number of Site Recovery Manager Server Log Files

You can change the size, number, and location of Site Recovery Manager Server log files.

You can modify the Site Recovery Manager log settings in the `vmware-dr.xml` configuration file on the Site Recovery Manager Server.

Procedure

1 Log in to the Site Recovery Manager Server host.

2 Open the `vmware-dr.xml` file in a text editor.

You find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder.

3 Find the `<log>` section in the `vmware-dr.xml` file.

4 Set the maximum size in megabytes of the logs to retain.

You set the maximum log size by adding a <maxFileSize> section to the <log> section. The default is 5 MB.

```
<log>

   <maxFileSize>5</maxFileSize>

</log>
```

5 Set the maximum number of log files to retain.

You set the maximum number of logs by adding a <maxFileNum> section to the <log> section. The default is 10 log files.

```
<log>

   <maxFileNum>50</maxFileNum>

</log>
```

6 Change the location on the Site Recovery Manager Server in which to store the logs.

You change the log location by modifying the <directory> section in the <log> section.

```
<log>

   <directory>C:\ProgramData\VMware\VMware vCenter Site Recovery
    Manager\Logs</directory>

</log>
```

7 Change the default prefix for log files.

You change the default prefix by modifying the <name> section in the <log> section.

```
<log>

   <name>vmware-dr</name>

</log>
```

8 Change the logging level.

You change the logging level by modifying the <level> section in the <log> section. The possible logging levels are error, warning, info, trivia, and verbose.

```
<log>

   <level>verbose</level>

</log>
```

9 (Optional) Set the level of logging for Site Recovery Manager Server components.

You can set specific logging levels for components by modifying the appropriate <level> sections. The possible logging levels are error, warning, info, trivia, and verbose. For example, you can set the logging level for a recovery to trivia.

```
<level id="Recovery">
   <logName>Recovery</logName>
   <logLevel>trivia</logLevel>
</level>
```

10 (Optional) Set the level of logging for storage replication adapters.

Setting the Site Recovery Manager logging level does not set the logging level for SRAs. You change the SRA logging level by adding a `<level id="SraCommand">` section to `vmware-dr.xml` to set the SRA logging level. The possible logging levels are error, warning, info, trivia, and verbose.

```
<level id="SraCommand">
   <logName>SraCommand</logName>
   <logLevel>trivia</logLevel>
</level>
```

11 Restart the Site Recovery Manager Server service for changes to take effect.

Configure Site Recovery Manager Core Dumps

You can configure Site Recovery Manager core dump settings to change the location of the core dump files and compress them.

You can modify the Site Recovery Manager core dump settings in the `vmware-dr.xml` configuration file on the Site Recovery Manager Server.

The Site Recovery Manager Server `rundll32.exe` child process monitors the primary Site Recovery Manager Server process for panic exits and is then responsible for generating the core dump.

Procedure

1 Log in to the Site Recovery Manager Server host.

2 Open the `vmware-dr.xml` file in a text editor.

You find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder.

3 Change the location on the Site Recovery Manager Server in which to store core dumps.

You change the core dump location by modifying the `<coreDump>` section.

```
<coreDump>C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles</coreDump>
```

The default path is `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles` unless this location does not exist or is not writable. In that case, Site Recovery Manager Server uses `C:\ProgramData\VMware`.

4 Use the core dump system parameters to limit the number of created and compressed dump files.

```
<debug>
  <dumpCoreCompression>true,false</dumpCoreCompression>
  <dumpFullCore>true,false</dumpFullCore>
</debug>
```

Option	Description
dumpCoreCompression	If unspecified, the default value is false. Site Recovery Manager Server does not compress previous core dump files as it creates core dump files. If you specify true, then Site Recovery Manager Server compresses all older core dumps when it generates a new core dump.
dumpFullCore	If unspecified, the default value is false. Site Recovery Manager Server generates a core dump file several MB in size and provides some assistance to support when a problem occurs. If you set this value to true, Site Recovery Manager Server generates a full core dump file that might be several GBs in size, depending on the workload at the time the core dump occurs. This larger file can provide greater assistance to support when a problem occurs. If disk space allows, set this value to true.

5 To modify the maximum number of core dump files, add a row to the <debug> section.

```
<maxCoreDumpFiles>max files</maxCoreDumpFiles>
```

If unspecified, the default value is 4. This value specifies the maximum number of core dump files that are retained in the core dump directory. When Site Recovery Manager Server createscore dumps, Site Recovery Manager Server deletes older files as necessary to avoid exceeding the maximum and consuming excessive disk space, especially when dumpFullCore is true.

Troubleshooting Site Recovery Manager 13

If you encounter problems with creating protection groups and recovery plans, recovery, or guest customization, you can troubleshoot the problem.

When searching for the cause of a problem, also check the VMware knowledge base at http://kb.vmware.com/.

This chapter includes the following topics:

Site Recovery Manager Doubles the Number of Backslashes in the Command Line When Running Callouts

When a backslash is a part of the callout command line, Site Recovery Manager doubles all backslashes.

Problem

The command-line system interpreter treats double backslashes as a single backslash only in file paths. If the callout command requires a backslash in a parameter other than a file path and the command does not convert double backslashes to a single backslash, the callout command might fail with an error.

For example, you can add a callout step to the workflow and enter the following text as a command:

```
c:\Windows\system32\cmd.exe /C "C:\myscript.cmd" a/b/c \d\e\f \\g\\h c:\myscript.log
```

As result of the callout step, Site Recovery Manager runs the following command:

```
c:\\Windows\\system32\\cmd.exe /C "C:\\myscript.cmd" a/b/c \\d\\e\\f \\\\g\\\\h c:\\myscript.log
```

If `myscript.cmd` does not change the double backslash to a single backslash, and parameters `\d\e\f` and `\\g\\h` are sensitive to the number of back slashes, `myscript.cmd` can fail.

Solution

1 Create an additional command-line batch file to contain commands and all required parameters. The callout step runs this additional batch file without any argument. For the example, the solution is as follows:

   a In a text editor such as Notepad, create a file `c:\SRM_callout.cmd` with the following content:
   `C:\myscript.cmd a/b/c \d\e\f \\g\\h c:\myscript.log`

   b In a recovery plan callout step, enter the command to run:
   `c:\\Windows\\system32\\cmd.exe /C c:\SRM_callout.cmd`

2 Add a code to the original script file that replaces double back slashes with a single back slash.

   a Add code similar to the following sample in the beginning of the script file `c:\myscript.cmd`.

   ```
   @echo off
   set arg2=%2
   set arg3=%3
   set fixed_arg2=%arg2:\\=\%
   set fixed_arg3=%arg3:\\=\%
   ```

   If you use the shift command in a script, all backslash-sensitive parameters are handled this way.

   b If you do not use the shift command in a script, make the following changes:

   Replace `%2` with `%fixed_arg2%`.

   Replace `%3` with `%fixed_arg3%`.

   c Do not change the callout step command.

Powering on Many Virtual Machines Simultaneously on the Recovery Site Can Lead to Errors

When many virtual machines perform boot operations at the same time, you might see errors during array-based and vSphere Replication recovery.

Problem

When powering on many virtual machines simultaneously on the recovery site, you might see these errors in the recovery history reports:

- `The command 'echo "Starting IP customization on Windows ..." > > % VMware_GuestOp_OutputFile %.`
- `Cannot complete customization, possibly due to a scripting runtime error or invalid script parameters.`
- `An error occurred when uploading files to the guest VM.`
- `Timed out waiting for VMware Tools after 600 seconds.`

Cause

By default, Site Recovery Manager does not limit the number of power-on operations that can be performed simultaneously. If you encounter errors while virtual machines power on on the recovery site, you can modify the `vmware-dr.xml` file to set a limit on the number of virtual machines that power on simultaneously.

If you encounter these errors, limit the number of power-on operations on the recovery site according to the capacity of your environment for a standalone host or for a cluster.

Solution

1. On the recovery server, go to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config`.
2. Open the `vmware-dr.xml` file in a text editor.
3. Update the `defaultMaxBootAndShutdownOpsPerCluster` and `defaultMaxBootAndShutdownOpsPerHost` values to limit the number of power-on operations at the recovery site.

   The following example shows how to limit the number of power-on operations to a maximum of 32 per cluster and 4 per standalone host.

   ```
   <config>
     <defaultMaxBootAndShutdownOpsPerCluster>32</defaultMaxBootAndShutdownOpsPerCluster>
     <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
   </config>
   ```

4. Restart the Site Recovery Manager Server service.

LVM.enableResignature=1 Remains Set After a Site Recovery Manager Test Recovery

Site Recovery Manager does not support ESXi environments in which the `LVM.enableResignature` flag is set to 0.

Problem

During a test recovery or an actual recovery, Site Recovery Manager sets `LVM.enableResignature` to 1 if the flag is not already set. Site Recovery Manager sets this flag to resignature snapshot volumes and mounts them on ESXi hosts for recovery. After the operation finishes, the flag remains set to 1.

Cause

Site Recovery Manager does not check how snapshot volumes are presented to ESXi hosts.
Site Recovery Manager does not support setting the `LVM.enableResignature` flag to 0. If you set the flag from 1 to 0, a virtual machine outage might occur each time you perform a test recovery or an actual recovery occurs.

Setting the `LVM.enableResignature` flag on ESXi hosts is a host-wide operation. When this flag is set to 1, during the host rescan or the next host reboot, all snapshot LUNs that are visible to the ESXi host, and that can be resignatured, are resignatured.

If snapshot volumes unrelated to Site Recovery Manager are forcefully mounted to ESXi hosts on the recovery site, these LUNs are resignatured as part of a host rescan during a test recovery or an actual recovery process. As a result, all the virtual machines in these volumes become inaccessible.

Solution

To prevent outages, make sure that no snapshot LUNs that are unrelated to Site Recovery Manager, and that are forcefully mounted, are visible to ESXi hosts on the recovery site.

Adding Virtual Machines to a Protection Group Fails with an Unresolved Devices Error

Adding virtual machines to a protection group fails with an error if you did not configure the appropriate inventory mappings.

Problem

When you add a virtual machine to a protection group, you see the error `Unable to protect VM 'virtual machine name' due to unresolved devices`.

Cause

You did not configure the inventory mappings to map the devices of the virtual machine on the protected site to the corresponding devices on the recovery site.

Solution

Configure the inventory mappings as described in *Site Recovery Manager Installation and Configuration*.

Configuring Protection fails with Placeholder Creation Error

When you configure protection on multiple virtual machines, the configuration fails with a placeholder creation error.

Problem

Configuring protection on a large number of virtual machines at the same time fails with either a placeholder creation timeout error or a placeholder creation naming error:

- `Placeholder VM creation error:Operation timed out:300 seconds`
- `Placeholder VM creation error:The name 'placeholder_name' already exists`

This problem occurs when you configure protection in different ways:

- You create a protection group that contains a datastore or datastores that contain a large number of virtual machines.
- You use the **Protection Groups > Virtual Machines > Restore All** option in the Site Recovery Manager interface on a large number of virtual machines.
- You use the Site Recovery Manager API to protect a large number of virtual machines manually.

Cause

The infrastructure on the recovery site is unable to handle the volume of concurrent creations of placeholder virtual machines.

Solution

Increase the `replication.placeholderVmCreationTimeout` setting from the default of 300 seconds. See "Change the Timeout for the Creation of Placeholder Virtual Machines," on page 107.

You do not need to restart Site Recovery Manager Server after changing this setting. Site Recovery Manager applies the setting the next time that you configure protection on a virtual machine.

Rapid Deletion and Recreation of Placeholders Fails

If you delete all of the placeholder virtual machines from a datastore, unmount the datastore, and remount the datastore, recreation of the placeholder virtual machines might fail.

Problem

Recreating the placeholders too rapidly after unmounting the datastore can fail with the error `NoCompatibleHostFound`.

Cause

The associations between ESXi hosts and datastores are updated at 10-minute intervals. If you recreate the placeholders after unmounting and remounting the datastore but before the next update, the host cannot be found.

Solution

Wait for more than 10 minutes after unmounting and remounting the datastore before you recreate the placeholder virtual machines.

Planned Migration Fails Because Host is in an Incorrect State

If you put the ESXi host on the recovery site into maintenance mode during a planned migration, the planned migration fails.

Problem

Planned migration fails with the error `Error – The operation is not allowed in the current state of the host`.

Cause

Site Recovery Manager cannot power on virtual machines on the recovery site when the ESXi host on the recovery site is in maintenance mode.

Solution

Exit maintenance mode on the ESXi host on the recovery site and rerun the planned migration.

Recovery Fails with a Timeout Error During Network Customization for Some Virtual Machines

During a recovery some virtual machines do not recover and show a timeout error during network customization.

Problem

During recovery some virtual machines do not recover within the default timeout period of 120 seconds.

Cause

This problem can occur for one of the following reasons.

- The VMware Tools package is not installed on the virtual machine that you are recovering.
- The cluster on the recovery site is experiencing heavy resource use while trying to simultaneously recover multiple virtual machines. In this case you can increase certain timeout settings to allow more time for tasks to complete. See "Change Recovery Settings," on page 105.

Solution

1 Verify that VMware Tools is installed on the virtual machine that you are recovering.

2 Check the available capacity on the recovery site.

If the recovery site is experiencing heavy resource use, increasing the timeout period for guest customization can resolve the issue.

a In the vSphere Web Client, click **Site Recovery > Sites**, select a site and click **Manage > Advanced Settings**.

b Select **Recovery** and click **Edit**.

c Increase the `recovery.customizationTimeout` parameter from the default of 600 seconds.

d Increase the `recovery.powerOnTimeout` parameter from the default of 300 seconds.

3 Run the recovery again.

Recovery Fails with Unavailable Host and Datastore Error

Recovery or test recovery fails with an error about host hardware and datastores being unavailable if you run the recovery or test shortly after changes occur in the vCenter Server inventory.

Problem

Recovery or test recovery fails with the error `No host with hardware version '7' and datastore 'ds_id' which are powered on and not in maintenance mode are available....`

Cause

Site Recovery Manager Server keeps a cache of the host inventory state. Sometimes when recent changes occur to the inventory, for example if a host becomes inaccessible, is disconnected, or loses its connection to some of the datastores, Site Recovery Manager Server can require up to 15 minutes to update its cache. If Site Recovery Manager Server has the incorrect host inventory state in its cache, a recovery or test recovery might fail.

Solution

Wait for 15 minutes before running a recovery if you change the host inventory. If you receive the error again, wait for 15 minutes and rerun the recovery.

Reprotect Fails with a vSphere Replication Timeout Error

When you run reprotect on a recovery plan that contains vSphere Replication protection groups, the operation times out with an error.

Problem

Reprotect operations on recovery plans that contain vSphere Replication protection groups fail with the error

```
Operation timed out: 7200 seconds VR synchronization failed for VRM
     group <Unavailable>. Operation timed out: 7200 seconds
```

.

Cause

When you run reprotect, Site Recovery Manager performs an online sync for the vSphere Replication protection group, which might cause the operation to timeout. The default timeout value is 2 hours.

Solution

Increase the `synchronizationTimeout` timeout value in Advanced Settings. See "Change vSphere Replication Settings," on page 110.

Recovery Plan Times Out While Waiting for VMware Tools

Running a recovery plan fails with a timeout error while waiting for VMware Tools to start.

Problem

Recovery operations fail at the Shutdown VMs step or Waiting for VMware Tools step of a recovery plan.

Cause

Site Recovery Manager uses VMware Tools heartbeat to discover when recovered virtual machines are running on the recovery site. Recovery operations require that you install VMware Tools on the protected virtual machines. Recovery fails if you did not install VMware Tools on the protected virtual machines, or if you did not configure Site Recovery Manager to start without waiting for VMware Tools to start.

Solution

Install VMware Tools on the protected virtual machines. If you do not or cannot install VMware Tools on the protected virtual machines, you must configure Site Recovery Manager not to wait for VMware Tools to start in the recovered virtual machines and to skip the guest operating system shutdown step. See "Change Recovery Settings," on page 105.

Synchronization Fails for vSphere Replication Protection Groups

During test recovery, planned migration, and reprotect of recovery plans that contain vSphere Replication protection groups, the virtual machine synchronization step fails with an error.

Problem

Synchronization of virtual machines in a vSphere Replication protection group fails with the error message `Error – VR synchronization failed for VRM group <Unavailable>. The object has already been deleted or has not been completely created.`

Cause

Excessive I/O traffic on one or more of the virtual machines in the protection group causes the synchronization to time out before it can finish. This can be because of heavy traffic. For example, setting the logging level to trivia mode can generate heavy I/O traffic.

Solution

1 Log in to the Site Recovery Manager Server host.

2 Open the `vmware-dr.xml` file in a text editor.

You find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder.

3 Add a <topology><drTaskCleanupTime> element to the vmware-dr.xml file.

You can add the <topology> element anywhere at the top level in the <Config> tags. Set the value of <drTaskCleanupTime> to at least 300 seconds. If you set the logging level to trivia, set <drTaskCleanupTime> to 1000 seconds.

```
<topology>
   <drTaskCleanupTime>1000</drTaskCleanupTime>
</topology>
```

4 Save and close the vmware-dr.xml file.

5 Restart the Site Recovery Manager Server service to apply the new settings.

Reprotect Fails After Restarting vCenter Server

After you restart vCenter Server, when you use vSphere Replication, reprotect operations sometimes fail.

Problem

After you restart vCenter Server, when you use vSphere Replication, reprotect operations fail with the error

```
Error – Unable to reverse replication for the virtual machine
     'virtual_machine'. The session is not authenticated.
```

Cause

After vCenter Server restarts, it fails to refresh some sessions that Site Recovery Manager uses to communicate with vSphere Replication and causes reprotect to fail.

Solution

Restart the Site Recovery Manager services on both of the sites.

Rescanning Datastores Fails Because Storage Devices are Not Ready

When you start a test recovery or a recovery, some SRAs send responses to Site Recovery Manager before a promoted storage device on the recovery site is available to the ESXi hosts. Site Recovery Manager rescans the storage devices and the rescan fails.

Problem

If storage devices are not fully available yet, ESXi Server does not detect them and Site Recovery Manager does not find the replicated devices when it rescans. This can cause several problems.

- Datastores are not created and recovered virtual machines cannot be found.
- ESXi hosts become unresponsive to vCenter Server heartbeat and disconnect from vCenter Server. If this happens,vCenter Server sends an error to Site Recovery Manager and a test recovery or real recovery fails.
- The ESXi host is available, but rescanning and disk resignaturing exceed the Site Recovery Manager or vCenter Server timeouts, resulting in a Site Recovery Manager error.

Cause

The storage devices are not ready when Site Recovery Manager starts the rescan.

Solution

To delay the start of storage rescans until the storage devices are available on the ESXi hosts, increase the `storageProvider.hostRescanDelaySec` setting to a value between 20 and 180 seconds. See "Change Storage Provider Settings," on page 108.

NOTE In Site Recovery Manager 5.1 and earlier, you might have used the `storageProvider.hostRescanRepeatCnt` parameter to introduce a delay in recoveries. Use the `storageProvider.hostRescanDelaySec` parameter instead.

Index